

# RFP #25-191

## Polk County South & Central County Jail Security Upgrades

Submitted by:

The Design Build Partnership of

**Driven Security & Johnson Controls**

241 Wilson Pike Circle  
Brentwood, TN 37027

10500 University Center Dr, Suite 275  
Tampa, FL 33612



Sealed Proposal. DO NOT OPEN	
<b>RFP Number</b>	25-191
<b>RFP Title</b>	Polk County South & Central County Jail Security Upgrades
<b>Due Date/Time:</b>	April 23, 2025, prior to 2:00 pm
<b>Submitted by:</b>	
<b>Deliver To:</b>	Polk County Procurement Division 330 West Church Street, Room 150, Bartow, Florida 33830



## TAB 1

### Executive Summary

Driven Security and Johnson Controls are premier companies within the security industry forming a strategic design-build partnership to provide a complete integrated security system for the facilities of Polk County. Together our companies provide almost 150 years of experience transforming facilities with award-winning technologies. We recognize that no one product or technology can address all of your security needs, so we offer a multi-tiered, multi-technology approach that combines leading-edge services and systems in an integrated environment that can lower the total cost of ownership.

Prisons and other correctional facilities seeking a total facility-wide solution have the opportunity to standardize on a single network-based platform that can streamline communications and provide interoperability, manageability and scalability. With our planning, layout, connected solutions, installation and support experience, we can offer a security system robust enough to handle the rigors and complexities of today's criminal justice operations. Our solutions are backed by experts who strive for excellence. When we work with a criminal justice facility, our team is committed to devising the best security solution, deploying it with attention to quality and providing excellent service and support.

When you are upgrading existing security capabilities and meeting new operational or regulatory requirements, we can be just what you need in your partners. With our wealth of equipment installation experience at criminal justice facilities, we know firsthand the infrastructure requirements of the industry. To help you safeguard your criminal justice facility with an advanced integrated security solution, we bring a wide array of capabilities together – needs analysis, planning, system layout, installation, integration, commissioning and uninterrupted support services.

We can combine leading technologies with customized design-build services in an integrated environment. It's a multi-tiered, multi-technology approach that recognizes no one product or application can address all of today's threats, and with the help of our value-oriented methodology, you can explore and implement innovations aimed at lowering costs, improving efficiency, enhancing security and anticipating future needs. Together we provide a unique and highly specialized team that can manage the planning, layout, installation and commissioning of your project.

Driven Security is a leading security technology company specializing in cloud-based physical security solutions tailored for law enforcement, commercial, educational, industrial, and municipal organizations. Driven's headquarters is in Brentwood, Tennessee and they have additional offices in Phoenix, Huntsville, Tampa, and Austin. Driven serves clients across the United States and offers a range of services for correctional facilities such as hybrid cloud-based video surveillance, intrusion detection, specialty enclosures and fencing solutions, barricades, security laminates, automated access control systems,





and security threat assessments. Driven partners with industry leaders such as Verkada for hybrid cloud-based platforms, ZeroEyes AI-driven weapon detection, and CEIA metal detection solutions. Driven is the largest provider of Verkada equipment to law enforcement facilities in the country and currently has a Platinum Verkada Reseller status. Driven's team has collectively completed over \$1B of construction projects.

Johnson Controls is a global leader in smart, healthy, and sustainable building technologies. Founded in 1885 by Warren S. Johnson, the company has extensive experience in innovating building solutions. Johnson Controls employs over 100,000 people across more than 150 countries. The company offers a comprehensive portfolio of products and services, including HVAC equipment, building automation systems, fire detection and suppression, and security solutions. Johnson Controls is an industry leader in correctional facility security. Johnson Controls is an industry leader in correctional facility security. The team is well versed in software and camera integration, PLC's, locking control systems, and all phases of the project from design all the way through commissioning and training for the project. Johnson Controls is currently active in over 175 criminal justice facilities in the United States. Many of these facilities are among the largest in the country. Johnson Controls initiatives include upgrading outdated infrastructures with modern systems such as video surveillance, access control, fire detection, and suppression systems. These efforts aim to improve safety, operational efficiency, and emergency response capabilities within correctional environments.

Together our companies can offer a comprehensive solution that meets or exceeds the needs and requests presented in this RFP. We bring a track record of excellence in secure facility upgrades backed by a depth of experience in law enforcement, municipal, and detention environments ensuring that Polk County receives a future-ready, fully compliant, and expertly managed design-build solution. Your county desires to unify your security platform across all facilities, while being stewards of the funds available to you. Our teams are prepared and uniquely qualified to unify your systems, manage the costs by value engineering your solution through the design build process and deliver an integrated security solution that will service your collective teams and environments as your county grow into the future.

## Driven Security

Adam Birdwell, PE  
241 Wilson Pike Circle  
Brentwood, TN 37027

[adam@drivenlocks.com](mailto:adam@drivenlocks.com)

615.533.4503

[www.drivenlocks.com](http://www.drivenlocks.com)

## Johnson Controls

Kevin Jones  
5757 N Green Bay Ave  
Milwaukee, WI 53209

[kevin.2.jones@jci.com](mailto:kevin.2.jones@jci.com)

334.399.2997

[www.johnsoncontrols.com](http://www.johnsoncontrols.com)

Polk County a Political Subdivision of the State of Florida - Vendor Security Questionnaire (Version 4.0)

The Polk County BoCC Information Technology Division, when considering any IT hardware/software solution, must ensure that due diligence is taken to validate that we are in compliance with local, state and national statutes and guidelines. When considering a technical purchase please complete the vendor identification section below and then respond to all questions and provide supporting documentation as requested. If documents are requested please click on the appropriate "Vendor Response" column. Please Leverage the "Dropdown" button for each question. Click "Insert" tab on Ribbon, Click "Object" button in "Text" group, and then select the appropriate file(s) to support the response for every request or question in each row. Please ensure each file is submitted in PDF format. Control References, where applicable, have been provided to assist with each request or question. Please provide any additional comments in the "Vendor Comments" column.



Vendor Name:	Verkada
Vendor Contact:	Driven Security - Adam Birdwell
Vendor Phone:	6155334503
Vendor Email:	<a href="mailto:adam@drivenlocks.com">adam@drivenlocks.com</a>
Project Name:	RFP 25-191 Polk County South & Central County Jail Security Upgrades
Date Completed:	4/30/2025

#	Question	Vendor Response	Vendor Comments
1	Document Requests and Information Security Policies		
1.1	Please attach a copy of your current Cyber liability insurance and Professional Liability insurance policies	Attached	Current insurance certificate available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
1.2	Does the vendor have individual(s) that are responsible for their IT Security Program?	Not attached (Please explain in "Vendor Comments")	Kyle Randolph is our Chief Information Security Officer.
1.3	Does the vendor have a Risk Management Program that includes IT related risks?	Attached	Verkada has a risk management program that is based on NIST 800-30 Guide for Conducting Risk Assessments. Verkada's Risk Management Policy is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .
1.4	Does the vendor have a SOC2 audit report covering application controls?	Attached	Verkada's SOC 2 Type 2 report available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
1.5	Please attach a copy of your latest penetration test and/or vulnerability assessment report	Attached	Verkada performs independent security assessments of the Command platform at least twice per year. An executive summary of the most recent assessment may be accessed at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
1.6	Does the solution involve a vendor or other third party transmitting, processing or storing protected health information (PHI)? Has a Business Associate Agreement been signed?	Attached	For an overview of our HIPAA compliance measures and how Verkada ensures the protection of sensitive data, please see our HIPAA documentation here: <a href="https://docs.verkada.com/docs/hipaa-compliance.pdf">https://docs.verkada.com/docs/hipaa-compliance.pdf</a>

1.7	Is the solution designed to comply with PCI, HIPPA, CJIS and other requirements?	Attached	<ul style="list-style-type: none"><li>– Our solution is designed to support/comply with PCI, CJIS, and HIPPA – Verkada does not manage any payment card data</li><li>– Verkada has a significant number of customers, including retail stores and banks, for which it plays a key role in helping those customers maintain PCI compliance with respect to both physical and cyber security.</li><li>– Verkada provides full access control event history (retained beyond the minimum PCI requirement of 90 days) that can automatically sync with Verkada camera footage. This event history can be easily examined, filtered, and exported to send to any recipient or external system. You can configure automatic alerting to send a notification (including over SMS and email) when an event occurs that meets your alerting criteria.</li><li>– Verkada meets and exceeds the high cybersecurity bar needed by PCI-compliant organizations:</li><li>– Verkada systems do not have vendor provided default passwords; SAML/OAuth and 2-factor authentication are available as standard options.</li><li>– Verkada automatically logs all user access and sessions via audit logs, which cannot be tampered with or altered. These audit logs are backed up into geographically redundant data centers.</li><li>– Verkada systems accurately record date and time, using the industry-standard Network Time Protocol (NTP).</li><li>– Verkada enables authorized administrators to review live and historical access control statuses and events on any device at any time, and to export this data on-demand or on a predetermined schedule.</li><li>– For more information on how Verkada helps support PCI compliance please click <a href="#">HERE</a>.</li></ul>
1.8	Does the vendor outsource management or support of the solution?	Not applicable	<p>Verkada customer support is available 24/7, details here. They can be contacted via the live chat functionality present within command, email or by phone. Product support is included with the cloud license and is available throughout the 10 year warranty period. Services include troubleshooting any challenge that a customer may have with their camera as well as overnight shipping of a new device if the camera is inoperable and covered under warranty. 24/7 Service is achieved by support representatives in Australia, London, and USA.</p> <p>The support team are direct employees and are primarily located in San Mateo, CA at Verkada HQ.</p> <p>Management of the solution is a customer and/or installation partner responsibility</p>

1.9	Does the vendor have processes to monitor changes to regulations, and to implement applicable changes in a timely manner?	Not attached (Please explain in "Vendor Comments")	<p>Privacy is fundamental to our philosophy. We have diligently endeavored to integrate privacy considerations into the design and development of our products and services. This approach ensures that our platforms deliver the security and functionality desired by our customers while respecting the privacy of individuals interacting with their organizations. Our steadfast commitment to privacy is guided by core principles: ownership, controls, privacy by default, transparency, and data minimization.</p> <p>Verkada aligns its privacy practices with the standards set by US state privacy laws. Acting as a data processor for customer personal data, Verkada utilizes Standard Contractual Clauses to establish a legal basis for transferring personal data from the EU/UK to the US.</p> <p>Furthermore, Verkada has disabled face detection and "person of interest notifications" in four US jurisdictions with regulations restricting private entities' use of facial recognition technology. These jurisdictions encompass Texas, Illinois, Baltimore (Maryland), and Portland (Oregon).</p>
1.10	Does the security design of the solutions infrastructure allow for segregation of each customer's application environment and data?	Attached	<p>The Verkada cloud solution is a multi-tenant application that implements security boundaries and individual keys per customer to ensure there is no commingling of data. Customer data is separated using logical access controls based on organization ID. Entities in the Verkada solution (organizations, users, cameras) are identified by cryptographically unguessable UUIDs, cameras belong to organizations, users are affiliated with organizations. User tokens are tied to the Org ID and associated keys, ensuring that no data outside of the user's organization can be decrypted or viewed. Only users affiliated with an organization explicitly can access the organization data.</p> <p>Architecture Info can be found at the below link: <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a></p>
2	Asset Management		
2.1	Do you maintain an inventory of all hardware and software assets, including ownership?	Yes	<p>Yes, Assets are classified in terms of business criticality, service-level expectations, and operation continuity requirements. A complete inventory of business-critical assets located at all sites and their usage over time are maintained and updated regularly.</p> <p>Policies and procedures also exist for the secure disposal of equipment.</p>
2.2	Do you have an information classification scheme and process designed to ensure that information is protected according to its confidentiality requirements?	Yes	<p>Client data in the form of video and audio is stored on the Verkada cameras themselves and stored for a retention period of 30, 60, 90, 120, 365 days based on hardware model. This camera footage can be backed up to the cloud on a per camera basis as necessary. Given this backup is uplink bandwidth intensive, this backup can be scheduled by the administrator ( <a href="https://help.verkada.com/en/articles/2452653-cloud-backup">https://help.verkada.com/en/articles/2452653-cloud-backup</a> )</p> <p>Client data in the AWS cloud is redundantly stored across isolated AWS Availability Zones providing redundancy for the data as well as high availability of the application. Backups of customer data stores are performed daily to an isolated AWS account for backups using AWS Backup.</p>
2.3	Do you maintain an inventory or map of data flows between both internal and external information systems?	Yes	Diagrams available in <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .

3	<b>Governance</b>		
3.1	Do you have an information security policy that has been approved by management and communicated to all applicable parties?	Yes	Information Security policies are reviewed and updated annually by the Security and Privacy Governance Committee, which includes the CISO, VP of Product, CTO, CFO and General Counsel. The policies are available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
3.2	Do you have an information security policy exception process that includes formal acceptance of risk by the risk owner?	Yes	Verkada has a risk management program that is based on NIST 800-30 Guide for Conducting Risk Assessments. Verkada's Risk Management Policy is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .
3.4	Do you regularly perform security threat and risk assessments on critical information systems using an industry-standard risk assessment methodology?	Yes	Verkada performs periodic penetration tests both via internal personal and third parties. Third Party Pen Tests are performed quarterly. An executive summaries of the most recent independent assessments is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
3.5	Have you designated an individual, who is at least at a manager level, who is responsible for information security activities?	Yes	Kyle Randolph is our Chief Information Security Officer.
4	<b>Supply Chain Risk Management</b>		
4.1	Do you perform security assessments on potential suppliers prior to entering into agreements with them?	Yes	Verkada reviews the SOC 2 reports annually of its service providers that store or process customer product data.
4.2	Do your agreements with suppliers include appropriate measures designed to meet security requirements?	Yes	Verkada has a vendor management program which is governed by the Verkada Vendor Risk and Compliance Management Policy. Critical vendors are re-assessed yearly according to the Verkada Risk Management Policy. Both policies are available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .
4.3	Do you regularly evaluate suppliers to ensure that they are meeting their security obligations?	Yes	Verkada reviews the SOC 2 reports annually of its service providers that store or process customer product data.
5	<b>Identity Management, Authentication, and Access Control</b>		
5.1	Is all access to information systems formally approved by the appropriate asset owner?	Yes	For the Command platform, new users must be invited by an Organization Administrator specific to that company's Organization in order to access Command.  For Verkada workforce members' access to Verkada's production systems and applications, there is a formal request and approval process for granting access to systems and applications.
5.2	Can all access to information systems be traced to unique individuals?	Yes	Yes. Audit logs are maintained at both the Organization (user / login) level as well as on specific cameras. The timestamp of the action, IP address of the user, username of the user and action taken are logged. Full details of all actions logged can be found here: <a href="https://help.verkada.com/en/articles/2729935-audit-logs">https://help.verkada.com/en/articles/2729935-audit-logs</a>
5.3	Are all access rights to information systems regularly reviewed for appropriateness by the asset owners?	Yes	Access reviews for critiical systems are performed quarterly. quarterly for internal employees. Clients manage access to their organization in Command.  Verkada's solution provides reporting interfaces for customers to review their own system owners and users access.
5.4	Are all access rights to information systems immediately revoked upon employee/contractor termination or change of role?	Yes	Access management is automated and immediate at the time of Verkada personnel offboarding and role transition.  Customers can implement the same functionality via SSO/SAML configuration

5.5	Do you restrict and control the use of privileged accounts through the use of a Privileged Account Management system or equivalent controls?	Yes	<p>Yes.</p> <p>Verkada audits &amp; logs a variety of security controls to detect anomalous admin/privileged account activity, which include, but are not limited to:</p> <ul style="list-style-type: none"> <li>– authentication activity for zero trust network access (which is required to access backend Verkada systems &amp; data)</li> <li>– Just-in-time, time-limited access request system (Verkada engineers are required to file requests via this system to obtain temporary privileged access to systems &amp; data)</li> <li>– This includes requests, reviews, approvals, and revocations</li> <li>– Authentication, onboarding &amp; offboarding from corporate single sign-on (SSO)</li> <li>– Activity from AWS KMS &amp; IAM</li> </ul> <p>This activity is logged &amp; stored in Verkada's SIEM. Detections &amp; alerts on these logs are written by Verkada's Detection &amp; Response team.</p>
5.6	Do you manage access permissions and authorizations, incorporating the principles of least privilege (or "need to know") and separation of duties?	Yes	<p>Verkada has full integration with SAML 2.0 authentication methods such as Okta/Duo/Active Directory/OneLogin. Additionally, Verkada supports SCIM integration that allows users to be provisioned from a central database with user permissions. For more information on SCIM integration and SAML, please reference the following link: <a href="https://help.verkada.com/en/articles/1132395-user-authentication-and-provisioning">https://help.verkada.com/en/articles/1132395-user-authentication-and-provisioning</a> and this article for details on role-based access controls in Command <a href="https://help.verkada.com/en/articles/4148620-roles-and-permissions-for-command">https://help.verkada.com/en/articles/4148620-roles-and-permissions-for-command</a></p>
5.7	Does the solution operate on the premise that "access that is not explicitly authorized is forbidden"?	Yes	<p>Yes all credentials for access to production systems are configured with the least privilege and following best practice. Authorized Verkada staff are permitted to access and view system information only for the purpose of troubleshooting and software development and only with customer approval. Verkada operates on a least privilege model, limiting the access to core system administrative accounts</p>
5.8	Do you require the use of multi-factor authentication for all remote access to organizational data, including email?	Yes	<p>Verkada can be set up to require user authentication through an organization's IDP, including Microsoft Azure, Okta, OneLogin, Google Workspace, ADFS, and Jumpcloud, with any multi-factor authentication options provided by the IDP. In addition, if authentication is performed directly with Verkada (and not through an IDP), users can set up multi factor authentication via security key, authenticator app or SMS. Details at <a href="https://help.verkada.com/en/articles/3831845-enable-2fa-for-your-command-account">https://help.verkada.com/en/articles/3831845-enable-2fa-for-your-command-account</a>. MFA is optional by default, but can be set as required for the organization. For more information please see our <a href="#">Authentication and Provisioning Overview</a>.</p>
5.9	Do you require the use of multi-factor authentication for all administrative access to cloud-based information systems?	Yes	<p>Verkada employees are required to use multifactor authentication including hardware keys.</p> <p>Customers have the ability to enable Two Factor Authentication for their accounts via SMS or through an authenticator app in order to login. <a href="https://help.verkada.com/en/articles/1132395-authentication-and-provisioning-overview">https://help.verkada.com/en/articles/1132395-authentication-and-provisioning-overview</a></p>
5.10	Does the solution have a configurable, automatic logoff feature after a period of inactivity?	Yes	<p>Command in a web browser has an Administrative configurable Org wide setting for Session Timeout Duration to force users to reauthenticate after a set period of time. The mobile Command app has the ability to configure app security where reauthentication is required after 15 minutes.</p>



5.11	Does the solution allow for restriction of access based on source IP address?	Yes	The Verkada solution can integrate with SSO solutions via SAML. When implemented, IP based restriction can be enforced via SAML.
5.12	Does the solution support the use of complex passwords?	Yes	Passwords are held to security guidelines: 8 characters minimum; 1 number, 1 symbol, 1 alpha; does not contain email; no reuse allowed.  The Verkada solution can integrate with SSO solutions via SAML. When implemented, expirations can be enforced via SAML.
5.13	Does the solution include configurable account lockout settings?	Yes	Yes, the Verkada solution implements a user lockout after 7 failed attempts. The lockout period is 15 minutes. Administrators do not have the ability to unlock a user account.
5.14	Are the Passwords unreadable during login?	Yes	Passwords are not able to be read by default during login.
5.15	Are all "default" passwords changed during system installation?	Not applicable (Please explain)	All passwords are explicitly set by the user at the time of implementation. No default passwords are in use.
6	Human Resource Security & Unauthorized Access to Data		
6.1	Do you have an information security awareness program designed to ensure that all employees and contractors receive security education as relevant to their job function?	Yes	Employees receive initial security training on date of employment and annually. Additionally, Verkada conducts ongoing security and privacy awareness training. Topics include: – How Common is Cybercrime? – Threats and Red Flags – Phishing – Social Media Sharing – Fake Profiles – Pretexting – Disinformation – Internet-Based Attacks – Tailgating – Lock Workstations/Clean Desk – Quiz
6.2	Do you conduct regular phishing simulation tests of your employees?	Yes	Employees receive initial security training on date of employment and annually. Additionally, Verkada conducts ongoing security and privacy awareness training. Topics include: – How Common is Cybercrime? – Threats and Red Flags – Phishing – Social Media Sharing – Fake Profiles – Pretexting – Disinformation – Internet-Based Attacks – Tailgating – Lock Workstations/Clean Desk – Quiz

6.3	Do you conduct appropriate background checks on all new employees based on the sensitivity of the role that they are being hired for?	Yes	<p>Verkada performs background checks at the time of hiring all employees and contractors.</p> <p>Background checks, depending on region, will include:</p> <ul style="list-style-type: none"><li>– United States</li><li>– County Criminal Court Search - 7 Years - Up to 3 Counties</li><li>– Domestic Watch List Search</li><li>– Social Security Number Trace</li><li>– Nationwide Criminal Databases Search</li><li>– Sex Offender Registry Search</li><li>– Canada</li><li>– RCMP Criminal Check &amp; ID Verification</li><li>– Other regions</li><li>– No check at this time</li></ul>
6.4	Do you require all new employees and contractors to sign confidentiality agreements?	Yes	All Verkada employees and contractors must sign a confidentiality agreement.
6.5	Does the vendor's workforce understand their responsibilities regarding the copying and disclosing of sensitive information?	Yes	<p><b>At Employment Onboarding:</b> All employees are required to sign an NDA as a part of their onboarding process. This is done to safeguard sensitive information and proprietary data they may have access to during their employment.</p> <p><b>Contractors:</b> Before starting work, all contractors are required to sign NDAs. This ensures that even though they are not permanent employees, they are still obligated to maintain the confidentiality of the company's sensitive information they may come in contact with.</p> <p><b>Third-Party and Hosted Data Centre Providers:</b> All third-party vendors, including hosted data center providers, are required to sign an NDA before engaging in business with our company. This is a crucial step given they might have access to critical company data. The NDA aims to secure any information that is shared with them and restrict unauthorized use or disclosure.</p> <p><b>Partnerships and Collaborations:</b> During strategic partnerships, collaborations, or business agreements, NDAs are signed to protect the proprietary and confidential information that might be shared between the organizations.</p>
7	<b>Data Security</b>		
7.1	Do you require that all removable media, which may contain organizational data, is encrypted?	Not applicable (Please explain)	Technical controls are in place to forbid the use of removable media.



7.2	Do you require that all media, including hardcopies, containing organizational data is disposed of securely when no longer required?	Yes	<p>Yes, all Verkada storage media must be given to Verkada IT for disposal and all storage media will be sanitized prior to disposal.</p> <p>For the camera footage, Verkada may, upon a written request from a customer's authorized account administrators, decommission a camera -- or camera. The decommissioning request must be made within the administrator's authenticated Verkada Offering environment. Once processed, this request will permanently delete all the data stored on the device and restore the hardware to its factory-set defaults.</p> <p>Within the AWS infrastructure, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 as part of the decommissioning process.</p>
7.3	Have you implemented data loss prevention tools?	Not applicable (Please explain)	All production endpoint devices have mandatory encryption for storage and strict role based access and time restrictions to limit data exfiltration.
7.4	Do you secure sensitive data at rest? (e.g. full disk encryption on all laptops, database encryption, salted and hashed passwords)	Yes	All data stored on the camera is AES 128-bit encrypted and all data stored in AWS is 256-bit encrypted.
8	<b>System &amp; Software Acquisition, Development, &amp; Change Control</b>		
8.1	Are information security requirements defined for all new information systems, whether acquired or developed?	Yes	The Information Security policy and program is modeled after NIST CSF and takes into consideration NIST 800-53 rev 5, ISO 27002, and 2017 AICPA Trust Services Criteria for Security (aka SOC 2).
8.2	Are development and testing environments separate from the production environment?	Yes	Verkada separates its production environment from its development and test environments.
8.3	Are your applications developed with secure coding practices, including the OWASP Top 10 Most Critical Web Application Security Risks?	Yes	<p>Verkada runs web security scans at least weekly that cover the OWASP Top Ten.</p> <p>For code review Verkada implements segregation-of-duties across its SDLC as well as system management. All changes to the code base go through a peer code review process utilizing static analysis tools such as Semgrep. All software engineers must complete secure coding training that covers secure coding concepts, including OWASP top ten considerations.</p>

8.4	Are your web applications protected by an application layer firewall?	No	<p>Below are the reasons we do not implement WAF: We understand that WAFs are commonly used to enhance web security. Still, in our case, we have implemented a robust set of compensating controls that effectively mitigate the risks WAFs are typically designed to address. Here are the key reasons why a WAF is not required in our architecture:– <b>Built-in Web Security Protections</b> – Our application follows secure coding best practices, including <b>Content Security Policy (CSP), output encoding, and anti-CSRF token checks</b> to mitigate common web vulnerabilities such as XSS and CSRF. Additionally, our frontend is built using React, which output-encodes data by default, helping prevent cross-site scripting (XSS) attacks by ensuring untrusted data is properly sanitized before rendering.– <b>Proactive Vulnerability Management</b> – We implement <b>static code analysis, mandatory code reviews, web application security scanning, and cloud security posture management tools</b>. This approach ensures that vulnerabilities such as SQL injection, XSS, and other injection-based attacks are identified and mitigated before they reach production.– <b>Istio Gateway for Authentication &amp; API Security</b>—We leverage <b>an Istio gateway to enforce authentication and validate API paths</b>. This ensures that only authenticated traffic is allowed and that only published API endpoints can be accessed externally. It prevents unauthorized access and significantly reduces attack vectors that a WAF would typically protect against.– <b>AWS Native Security Measures</b> – Our architecture leverages <b>AWS Shield</b> for DDoS protection and <b>AWS Load Balancers</b> to distribute traffic securely. These services provide a foundational layer of security against volumetric attacks, ensuring high availability and resilience against malicious traffic.– <b>Custom Rate Limiting Implementation</b>—We have built an <b>in-house rate-limiting mechanism</b> to prevent abuse and limit excessive requests. This control complements our other security layers and protects against brute-force attacks and API misuse. With these comprehensive security controls in place, we ensure that our applications are effectively protected against web-based threats without needing a WAF.</p>
8.5	Do you incorporate threat modeling into application design?	Yes	
5.6	Is application source code tested for vulnerabilities using source code reviews or static and dynamic application security testing?	Yes	Verkada utilizes Static code analysis, mandatory code reviews, web application security scanning and cloud security posture management tools to identify and mitigate injection vulnerabilities.
8.7	Are new information systems scanned for vulnerabilities prior to deployment?	Yes	Vulnerability scans are run daily. Vulnerabilities are ticketed and fixed according to internal Service Level Objective timelines based on security severity.
8.8	Do you monitor and restrict the installation of unauthorized software?	Yes	We do not allow direct access to device interfaces and therefore do not allow additional software installation.
8.9	Does the vendor have separate development, test & production environments for programming?	Yes	Verkada separates its production environment from its development and test environments.
8.10	Is a detailed security testing of the application, including peer review, part of the software development process?	Yes	All code changes require peer review, including security code review.

8.11	Do change management procedures include testing & approval of code changes prior to implementation?	Yes	Verkada has a rigorous change management, update and deployment program in place. Updates are reviewed in mandatory peer code reviews, tested on internal test systems, then pushed to a set of “canary” devices on our production network. Next, users who opt in to our beta program receive updates, and then the update is pushed to the entire population. Verkada runs sweeps to update any new or re-connected devices that may not have received the original update. Verkada maintains a full audit log of all changes made to each device and to the system.
8.12	Does vendor conduct continuous testing to ensure that code changes to the application do not introduce vulnerabilities?	Yes	<p>– <b>Built-in Web Security Protections</b> – Our application follows secure coding best practices, including <b>Content Security Policy (CSP), output encoding, and anti-CSRF token checks</b> to mitigate common web vulnerabilities such as XSS and CSRF. Additionally, our frontend is built using React, which output-encodes data by default, helping prevent cross-site scripting (XSS) attacks by ensuring untrusted data is properly sanitized before rendering.</p> <p>– <b>Proactive Vulnerability Management</b> – We implement <b>static code analysis, mandatory code reviews, web application security scanning, and cloud security posture management tools</b>. This approach ensures that vulnerabilities such as SQL injection, XSS, and other injection-based attacks are identified and mitigated before they reach production.</p> <p>– <b>Istio Gateway for Authentication &amp; API Security</b>—We leverage <b>an Istio gateway to enforce authentication and validate API paths</b>. This ensures that only authenticated traffic is allowed and that only published API endpoints can be accessed externally. It prevents unauthorized access and significantly reduces attack vectors that a WAF would typically protect against.</p> <p>– <b>AWS Native Security Measures</b> – Our architecture leverages <b>AWS Shield</b> for DDoS protection and <b>AWS Load Balancers</b> to distribute traffic securely. These services provide a foundational layer of security against volumetric attacks, ensuring high availability and resilience against malicious traffic.</p> <p>– <b>Custom Rate Limiting Implementation</b>—We have built an <b>in-house rate-limiting mechanism</b> to prevent abuse and limit excessive requests. This control complements our other security layers and protects against brute-force attacks and API misuse.</p>
8.13	Does the vendor provide information regarding 3rd party applications that solution utilizes?	Not applicable (Please explain)	No third party software is required to deploy the Verkada surveillance solution.

8.14	Does the vendor use the minimum information or data necessary for solution setup & ongoing processing?	Yes	<p>Verkada can provide granular administrative levels for all sites as well as site-based individual privileges. There are four levels of access that a user or group may have to a site or sub-site:</p> <ul style="list-style-type: none"><li>– <b>Site Admin:</b> Permits users to view cameras, add cameras, archive and share video, change camera settings, create and delete archived videos, take snapshots, and edit site permissions.</li><li>– <b>Site Viewer:</b> Permits users to view cameras, create archived videos, and take snapshots.</li><li>– <b>Live-Only Viewer:</b> Permits users to only view camera live streams (no access to historical video, archives, or live link sharing).</li><li>– <b>No Access:</b> Users will have no access to the site or sub-site's camera live feeds, historical video, or archives.</li></ul> <p>For organization wide-access, you can create Org Admins. These roles will allow you access to all sites and sub-sites within the district. The role allows for the creation of other admins.</p> <p>Please find a roles and permissions overview <a href="#">here</a>.</p>
8.15	Does the vendor solution include de-identifying confidential data (if applicable) used for testing?	Not applicable (Please explain)	We do not associate analytics data with identifying information by default, the only identifying information that would be correlated with user data would be entered by the application owner.
8.16	Does the vendor environment utilize methods to detect & block application level software attacks?	Yes	<p>Yes.</p> <p>Verkada audits &amp; logs a variety of security controls to detect anomalous admin/privileged account activity, which include, but are not limited to:</p> <ul style="list-style-type: none"><li>– authentication activity for zero trust network access (which is required to access backend Verkada systems &amp; data)</li><li>– Just-in-time, time-limited access request system (Verkada engineers are required to file requests via this system to obtain temporary privileged access to systems &amp; data)</li><li>– This includes requests, reviews, approvals, and revocations</li><li>– Authentication, onboarding &amp; offboarding from corporate single sign-on (SSO)</li><li>– Activity from AWS KMS &amp; IAM</li></ul> <p>This activity is logged &amp; stored in Verkada's SIEM. Detections &amp; alerts on these logs are written by Verkada's Detection &amp; Response team.</p>
9	Physical and Environmental Security		
9.1	Are physical security perimeter controls implemented around sensitive locations such as data centers?	Yes	Physical security controls at the AWS data centers are detailed here: <a href="https://aws.amazon.com/compliance/data-center/controls/">https://aws.amazon.com/compliance/data-center/controls/</a>
9.2	Are all visitors appropriately identified, logged, and escorted while in sensitive locations?	Yes	All visitors are required to sign in at the front desk using Verkada's Guest product and are escorted by employees to non-public areas.
9.3	Does the physical controls for the data center facilities, include controls such as backup power supplies, generators, etc.?	Yes	Yes, details at <a href="https://aws.amazon.com/compliance/data-center/controls/">https://aws.amazon.com/compliance/data-center/controls/</a>

9.4	Does the vendor have policies & processes in place for the secure disposal and reuse of IT equipment?	Yes	<p>Yes, all Verkada storage media must be given to Verkada IT for disposal and all storage media will be sanitized prior to disposal.</p> <p>For the camera footage, Verkada may, upon a written request from a customer's authorized account administrators, decommission a camera -- or camera. The decommissioning request must be made within the administrator's authenticated Verkada Offering environment. Once processed, this request will permanently delete all the data stored on the device and restore the hardware to its factory-set defaults.</p> <p>Within the AWS infrastructure, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 as part of the decommissioning process.</p>
10	Information Protection Processes and Procedures		
10.1	Are security configuration baselines defined and implemented for all endpoints and network devices?	Yes	Verkada leverages Configuration-as-Code where possible for configuration management. All configuration-as-code changes must be peer reviewed. Manual changes are manually reviewed as part of a Change Management process.
10.2	Do you use automated tools to verify that endpoints and network devices comply with their baselines?	Yes	Verkada runs periodic firmware integrity checks on all cameras to ensure there hasn't been any tampering with our firmware and releases regular updates to its firmware. These updates enhance security and functionality, and they are included at no cost as part of your cloud license. To ensure failsafe updates, each Verkada device is equipped with a dual-partition firmware bank. If a device were to fail an automated check, our security team would be notified immediately and you are then contacted.
10.3	Do you segregate your network into zones based on trust levels, and control the flow of traffic between zones?	Yes	The Verkada cloud solution is a single multi-tenant application that implements security boundaries (logical access control based on organization ID) and individual keys per customer to ensure there is no commingling of data. Entities in the Verkada solution (organizations, users, cameras) are identified by unguessable UUIDs, cameras belong to organizations, users are affiliated with organizations. User tokens are tied to the Org ID and associated keys, ensuring that no data outside of the user's organization can be decrypted or viewed. Only users affiliated with an organization explicitly can access the organization data. This practice is a standard business practice.
10.4	Are all changes to information systems recorded, planned, and tested?	Yes	Modifications to the production environment are governed by the Change Management Standard.
10.5	Are all information systems that are susceptible to malware protected by up-to-date anti-malware software?	Yes	Verkada servers are hosted in AWS and run Linux. Linux is not a common target for viruses, so no antivirus. Server integrity and potential malware activity is monitored by Verkada's Cloud Security Posture Management tool.

10.6	Do you have a backup and recovery process designed to ensure that data can be recovered in the event of unexpected loss?	Yes	<p>Client data in the form of video and audio is stored on the Verkada cameras themselves and stored for a retention period of 30, 60, 90, 120, 365 days based on hardware model. This camera footage can be backed up to the cloud on a per camera basis as necessary. Given this backup is uplink bandwidth intensive, this backup can be scheduled by the administrator (<a href="https://help.verkada.com/en/articles/2452653-enable-cloud-backup">https://help.verkada.com/en/articles/2452653-enable-cloud-backup</a>). Camera video data backups may be stored in AWS or Backblaze B2 depending on the region configured for storage.</p> <p>Client data in the AWS cloud is redundantly stored across isolated AWS Availability Zones providing redundancy for the data as well as high availability of the application. Backups of customer data stores are performed daily to an isolated AWS account for backups using AWS Backup.</p>
10.7	Do you monitor external sources, such as vendor bulletins, for newly identified vulnerabilities and patches?	Yes	Vulnerability scans are run daily. Vulnerabilities are ticketed and fixed according to internal Service Level Objective timelines based on security severity.
10.8	Do you evaluate, test, and apply information system patches in a timely fashion according to their risk?	Yes	Vulnerabilities and Patches are fixed/applied according to Service Level Objective timelines specified in Verkada's Vulnerability Management Standard depending on their CVSS score and risk level.
<b>11</b>	<b>Data Protection &amp; Protective Technology</b>		
11.1	Have security event logging requirements been defined, and are all information systems configured to meet logging requirements?	Yes	Yes, Verkada monitors security logs and alerts in a SIEM.
11.2	Are security event logs protected and retained per defined logging requirements?	Yes	Security logs are retained for at least 365 days.
11.3	Have you deployed intrusion detection or prevention systems at the network perimeter?	No	Verkada has implemented compensating controls for network security and detection rules related to network security in its SIEM.
11.4	Have you deployed tools to limit web browsing activity based on URL categories?	No	All production endpoint devices have mandatory encryption for storage and strict role based access and time restrictions to limit data exfiltration.
11.5	Have you deployed controls to detect and mitigate denial of service attacks?	Yes	Verkada's AWS environment is protected by AWS Shield.
11.6	Are there management policies & procedures in place to protect the use & storage of cryptographic keys (PKI)?	Yes	The camera footage and data stored on the cameras themselves is encrypted using AES 128 encryption. Any data and footage stored in the Verkada AWS cloud (thumbnails, archived video, credentials, metadata) is encrypted using AES 256 encryption. Individual per camera encryption keys are managed using AWS Key Management Service (KMS: <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a> ). AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2. Keys are rotated monthly.
11.7	Does the solution securely transmit sensitive data over public networks (e.g. passwords, command shells, files with sensitive content, database connections, email encryption)?	Yes	All data, including login credentials and other sensitive data, are encrypted with TLS 1.2 or greater for all connections to the Command platform over public networks.
<b>12</b>	<b>Security Continuous Monitoring &amp; Login Auditing</b>		
12.1	Have you deployed automated tools to collect, correlate, and analyze security event logs from multiple sources for anomalies?	Yes	Yes, Verkada monitors security logs and alerts in a SIEM.
12.2	Are security alerts monitored 24x7?	Yes	Yes, Verkada monitors security logs and alerts in a SIEM.
12.3	Do you employ automated tools to scan information systems for vulnerabilities on a regular basis?	Yes	Vulnerability scans are run daily. Vulnerabilities are ticketed and fixed according to internal Service Level Objective timelines based on security severity.
12.4	Does the solution record all exceptions & security relevant events in application & system logs?	Yes	Audit logs are retained for 365 days. Customers may access the audit log for their organization in the Command platform.



12.5	Are all audit logs secure from modifications?	Yes	<p>Yes. Audit logs are maintained at both the Organization (user / login) level as well as on specific cameras. The timestamp of the action, IP address of the user, username of the user and action taken are logged. Full details of all actions logged can be found here:  <a href="https://help.verkada.com/en/articles/2729935-audit-logs">https://help.verkada.com/en/articles/2729935-audit-logs</a></p> <p>The logs are immutable on the web from a user perspective. They can be modified after downloading (CSV format)</p>
12.6	Are the application audit logs recorded?	Yes	<p>Yes. Audit logs are maintained at both the Organization (user / login) level as well as on specific cameras. The timestamp of the action, IP address of the user, username of the user and action taken are logged. Full details of all actions logged can be found here:  <a href="https://help.verkada.com/en/articles/2729935-audit-logs">https://help.verkada.com/en/articles/2729935-audit-logs</a></p>
12.7	Are the logs regularly reviewed to examine user ID's, dates & times of log on & log off, login failure events, etc.?	Yes	Yes, for more information on audit logs, please see the following : <a href="https://help.verkada.com/en/articles/2729935-audit-logs">https://help.verkada.com/en/articles/2729935-audit-logs</a>
12.8	Are the system logs reviewed at a defined frequency & retained for as long as required?	Yes	Audit logs are retained for 365 days. Customers may access the audit log for their organization in the Command platform.
<b>13</b>	<b>Information Security Incident Management &amp; Disclosure of Security Breaches</b>		
13.1	Do you have a formal, documented security incident response plan?	Yes	Verkada's Security Incident Response Plan is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
13.2	Do you conduct regular tests of your security incident response plan?	Yes	Verkada's security incident response plan is tested at least annually with tabletop exercises.
13.3	Are all security incidents recorded, classified, and tracked?	Yes	Yes, Verkada monitors security logs and alerts in a SIEM.
13.4	Are forensic investigations conducted as part of incident response?	Yes	Verkada's Security Incident Response Plan is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
13.5	Does the vendor have procedures to notify the Polk County BoCC IT Division following the discovery of a breach without reasonable delay?	Yes	If a Verkada security incident affects a customer, Verkada will notify that customer within 48 hours.
13.6	Does the disclosure notification include the identification of data & each individual whose private data has been, or is reasonably believed to have been accessed, acquired, or disclosed during the breach?	Yes	In the event of a breach or a suspected breach there will be emailed written notice sent to the client within 48 hours of discovery of the breach. This email shall include the identification of the dataset that was compromised and investigative details (if applicable). Verkada's incident response plan is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .
13.7	When a breach is discovered, does the vendor assign ownership of a breach for reporting purposes?	Yes	In the event of a breach or a suspected breach there will be emailed written notice sent to the client within 48 hours of discovery of the breach. This email shall include the identification of the dataset that was compromised and investigative details (if applicable). Verkada's incident response plan is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .
<b>14</b>	<b>Privacy</b>		
14.1	Do you have a data retention policy and process that is designed to meet relevant privacy regulations?	Yes	The Verkada cloud solution is a multi-tenant application that implements security boundaries and individual keys per customer to ensure there is no commingling of data. Customer data is separated using logical access controls based on organization ID. Entities in the Verkada solution (organizations, users, cameras) are identified by cryptographically unguessable UUIDs, cameras belong to organizations, users are affiliated with organizations. User tokens are tied to the Org ID and associated keys, ensuring that no data outside of the user's organization can be decrypted or viewed. Only users affiliated with an organization explicitly can access the organization data.

14.2	Do you maintain an inventory and mapping of where all personal data is stored that includes cross-border data flows?	Yes	Diagrams available in <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a> .
<b>15</b>	<b>Disaster Recovery, Business Continuity &amp; System Availability</b>		
15.1	Does the vendor have a developed & documented Disaster Recovery and Business Continuity Plans?	Yes	Verkada's Disaster Recovery & Business Continuity plan is available at <a href="https://my.pima.app/p/verkada/verkada-standard-security-docs">https://my.pima.app/p/verkada/verkada-standard-security-docs</a>
15.2	Has the Disaster Recovery Plan been tested within the last year? If not, when?	No	Verkada's most recent Disaster Recovery test was completed in September 2023.
15.3	Does the solution have a disaster recovery plan and procedures?	Yes	<p>Client data in the form of video and audio is stored on the Verkada cameras themselves and stored for a retention period of 30, 60, 90, 120, 365 days based on hardware model. This camera footage can be backed up to the cloud on a per camera basis as necessary. Given this backup is uplink bandwidth intensive, this backup can be scheduled by the administrator (<a href="https://help.verkada.com/en/articles/2452653-enable-cloud-backup">https://help.verkada.com/en/articles/2452653-enable-cloud-backup</a>)</p> <p>Client data in the AWS cloud is redundantly stored across isolated AWS Availability Zones providing redundancy for the data as well as high availability of the application. Backups of customer data stores are performed daily to an isolated AWS account for backups using AWS Backup.</p> <p>Verkada has no limitations on the number of Cameras or products being added to the same site as we do not rely on a physical infrastructure like NVR or DVR. We are elastic and seamless therefore sky is the limit in terms of scalability and ease of deployment.</p>
15.4	Are the backups encrypted using 256 bit AES encryption or better?	Yes	Cloud backups utilize AES 256-bit encryption
<b>16</b>	<b>Anti-malware and Vulnerability Management</b>		
16.1	Does the solution support the use of anti-malware protection?	No	<p>Verkada servers are hosted in AWS and run Linux. Linux is not a common target for viruses, so no antivirus. Server integrity and potential malware activity is monitored by Verkada's Cloud Security Posture Management tool.</p> <p>Verkada is a cloud based solution and is not relevant the use of anti-malware protection for client machines.</p>
16.2	Does the vendor have processes to monitor & manage system vulnerabilities to mitigate malware?	Yes	Vulnerability scans are run daily. Vulnerabilities are ticketed and fixed according to internal Service Level Objective timelines based on security severity.
16.3	Does the vendor have a comprehensive patch & vulnerability management program to include internal systems as well as external services, software & products along with reliable customer notifications?	Yes	<p>Yes. Verkada uses recommended AWS tools and services for vulnerability detection and patch management. Patches are pushed out to the Verkada cameras on an as-needed basis. The devices continually query the Verkada firmware upgrade server and pull firmware automatically. Once downloaded the devices go through the following process to ensure they have received a valid firmware update. The device will confirm the source, run a health check and confirm that it is a committed release.</p> <p>Verkada's Command platform applies patches at all levels of the tech stack according to internal SLO timelines according to security severity.</p>
16.4	Does the vendor scan for system vulnerabilities on a continuous or regular basis?	Yes	Vulnerability scans are run daily. Vulnerabilities are ticketed and fixed according to internal Service Level Objective timelines based on security severity.



16.5	Does the vendor have procedures in place to determine if assets have been compromised?	Yes	<p>Yes.</p> <p>Verkada audits &amp; logs a variety of security controls to detect anomalous admin/privileged account activity, which include, but are not limited to:</p> <ul style="list-style-type: none"><li>– authentication activity for zero trust network access (which is required to access backend Verkada systems &amp; data)</li><li>– Just-in-time, time-limited access request system (Verkada engineers are required to file requests via this system to obtain temporary privileged access to systems &amp; data)</li><li>– This includes requests, reviews, approvals, and revocations</li><li>– Authentication, onboarding &amp; offboarding from corporate single sign-on (SSO)</li><li>– Activity from AWS KMS &amp; IAM</li></ul> <p>This activity is logged &amp; stored in Verkada's SIEM. Detections &amp; alerts on these logs are written by Verkada's Detection &amp; Response team.</p>
16.6	Does the vendor have a configuration management program?	Yes	<p>Verkada leverages Configuration-as-Code where possible for configuration management. All configuration-as-code changes must be peer reviewed. Manual changes are manually reviewed as part of a Change Management process.</p>
17	<b>Data Life Cycle Controls</b>		
17.1	Does the vendor agree to end of contract separation provisions related to data?	Yes	<p>Yes, all Verkada storage media must be given to Verkada IT for disposal and all storage media will be sanitized prior to disposal.</p> <p>For the camera footage, Verkada may, upon a written request from a customer's authorized account administrators, decommission a camera -- or camera. The decommissioning request must be made within the administrator's authenticated Verkada Offering environment. Once processed, this request will permanently delete all the data stored on the device and restore the hardware to its factory-set defaults.</p> <p>Within the AWS infrastructure, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 as part of the decommissioning process.</p>
17.2	Does the vendor have a defined process for secure disposal of customer's data?	Yes	<p>Yes, all Verkada storage media must be given to Verkada IT for disposal and all storage media will be sanitized prior to disposal.</p> <p>For the camera footage, Verkada may, upon a written request from a customer's authorized account administrators, decommission a camera -- or camera. The decommissioning request must be made within the administrator's authenticated Verkada Offering environment. Once processed, this request will permanently delete all the data stored on the device and restore the hardware to its factory-set defaults.</p> <p>Within the AWS infrastructure, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in NIST 800-88 as part of the decommissioning process.</p>



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

12/4/2024

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an **ADDITIONAL INSURED**, the policy(ies) must have **ADDITIONAL INSURED** provisions or be endorsed. If **SUBROGATION** IS **WAIVED**, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> Newfront Insurance Services 777 Mariners Island Blvd Suite 250 San Mateo, CA 94404  www.newfront.com	<b>CONTACT NAME:</b> Cert Request <b>PHONE (A/C, No, Ext):</b> 650-488-8565 <b>E-MAIL ADDRESS:</b> TechCertRequest@newfront.com <b>FAX (A/C, No):</b>														
<b>INSURED</b> Verkada Inc. 406 E 3rd Avenue San Mateo CA 94401	<table><tr><th>INSURER(S) AFFORDING COVERAGE</th><th>NAIC #</th></tr><tr><td>INSURER A: Federal Insurance Company</td><td>20281</td></tr><tr><td>INSURER B: Chubb National Insurance Company</td><td>10052</td></tr><tr><td>INSURER C: Associated Industries Insurance Company</td><td>23140</td></tr><tr><td>INSURER D: Westchester Surplus Lines Insurance Co</td><td>10172</td></tr><tr><td>INSURER E: AXIS Surplus Insurance Company</td><td>26620</td></tr><tr><td>INSURER F:</td><td></td></tr></table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: Federal Insurance Company	20281	INSURER B: Chubb National Insurance Company	10052	INSURER C: Associated Industries Insurance Company	23140	INSURER D: Westchester Surplus Lines Insurance Co	10172	INSURER E: AXIS Surplus Insurance Company	26620	INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: Federal Insurance Company	20281														
INSURER B: Chubb National Insurance Company	10052														
INSURER C: Associated Industries Insurance Company	23140														
INSURER D: Westchester Surplus Lines Insurance Co	10172														
INSURER E: AXIS Surplus Insurance Company	26620														
INSURER F:															

**COVERAGES****CERTIFICATE NUMBER:** 82907443**REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			3607-8334	12/1/2024	12/1/2025	EACH OCCURRENCE \$1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$1,000,000 MED EXP (Any one person) \$10,000 PERSONAL & ADV INJURY \$1,000,000 GENERAL AGGREGATE \$2,000,000 PRODUCTS - COMP/OP AGG \$2,000,000 \$
A	<input type="checkbox"/> <b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS ONLY			7362-9635	12/1/2024	12/1/2025	COMBINED SINGLE LIMIT (Ea accident) \$1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> <b>UMBRELLA LIAB</b> <input checked="" type="checkbox"/> <b>EXCESS LIAB</b> <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$0			7819-7246	12/1/2024	12/1/2025	EACH OCCURRENCE \$15,000,000 AGGREGATE \$15,000,000 \$
B	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N <input checked="" type="checkbox"/> N	N/A	7183-6878	9/1/2024	9/1/2025	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE - EA EMPLOYEE \$1,000,000 E.L. DISEASE - POLICY LIMIT \$1,000,000
C	Errors & Omissions/Cyber Liability			ACL1241256 01	12/1/2024	12/1/2025	Limit: \$5,000,000
D	Excess E&O/Cyber			G47439486 002	12/1/2024	12/1/2025	Limit: \$5,000,000
E	Excess E&O/Cyber			P-001-001299968-02	12/1/2024	12/1/2025	Limit: \$5,000,000

**DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES** (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Evidence of Insurance

**CERTIFICATE HOLDER**

Evidence of Insurance

**CANCELLATION**

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Rod Sockolov

Generated by Pima.app April 28, 2025 · 08:33 AM PDT

© 1988-2015 ACORD CORPORATION. All rights reserved.

ACORD 25 (2016/03)

The ACORD name and logo are registered marks of ACORD

# Risk Management Policy

## Purpose

The purpose of this policy is to define the methodology for the assessment and treatment of information security risks within Verkada, and to define the acceptable level of risk as set by Verkada's leadership.

## Scope

Risk assessment and risk treatment are applied to the entire scope of Verkada's information security program, and to all assets which are used within Verkada or which could have an impact on information security within it. This policy applies to all employees of Verkada who take part in risk assessment and risk treatment.

## Background

A key element of Verkada's information security program is a holistic and systematic approach to risk management. This policy defines the requirements and processes for Verkada to identify information security risks. The process consists of four parts: identification of Verkada's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

## Policy

### Risk Assessment

- The risk assessment process includes the identification of threats and vulnerabilities having to do with company assets.
- The first step in the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets which may affect the confidentiality, integrity, and/or availability of information in the organization. Assets may include documents in paper or electronic form, applications, databases, information technology equipment, infrastructure, and external/outsourced services and processes. For each asset, an owner must be identified.
- The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities must be listed in a risk assessment table. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities.
- For each risk, an owner must be identified. The risk owner and the asset owner may be the same individual.
- Once risk owners are identified, they must assess:

- Impact for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.
  - Likelihood of occurrence of such a risk (i.e. the probability that a threat will exploit the vulnerability of the respective asset).
  - Criteria for determining impact and likelihood are defined in the tables below.
- The risk level is calculated by multiplying the impact score and the likelihood score.

#### Description of Impact Levels and Criteria

Impact (Score)	Definition
Incidental (1.0)	• Minimal financial loss • Local media attention quickly remedied • Not reportable to regulator • Isolated staff dissatisfaction
Minor (2.0)	• Minor financial loss • Local reputational damage • Reportable incident to regulator, no follow up • General staff morale problems and increase in turnover
Moderate (3.0)	• Moderate financial loss • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Widespread staff morale problems and high turnover
Major (4.0)	• Significant financial loss • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
Extreme (5.0)	• Massive financial loss over \$50,000,000 • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Multiple senior leaders leave

#### Description of Likelihood Levels and Criteria

Likelihood (Weight Factor)	Definition
Rare (1.0)	Once in 100 years or less (<10% chance of occurrence over the life of the company)
Unlikely (2.0)	Once in 50 to 100 years (10% to 35% chance of occurrence over the life of the company)
Possible (3.0)	Once in 25 to 50 years (35% to 65% chance of occurrence over the life of the company)
Likely (4.0)	Once in 2 to 25 years (65% to 90% chance of occurrence over the life of the company)

	company)
Almost Certain (5.0)	Up to once in 2 years or more (90% or greater chance of occurrence over the life of the company)

### Risk Rating Criteria

<b>Risk Rating:</b>
<b>Low Risk:</b> Less than or equal to 4.0
<b>Medium Risk:</b> Greater than 4.0 but less than or equal to 9.0
<b>High Risk:</b> Greater than 9.0 but less than or equal to 16.0
<b>Critical Risk:</b> Greater than 16.0

### Risk Rating Matrix

RISK SCORE MATRIX						
		Impact				
		INCIDENTAL (1.0)	MINOR (2.0)	MODERATE (3.0)	MAJOR (4.0)	EXTREME (5.0)
Likelihood	RARE (1.0)	LOW $1.0 \times 1.0 = 1.0$	LOW $1.0 \times 2.0 = 2.0$	LOW $1.0 \times 3.0 = 3.0$	MEDIUM $1.0 \times 4.0 = 4.0$	MEDIUM $1.0 \times 5.0 = 5.0$
	UNLIKELY (2.0)	LOW $2.0 \times 1.0 = 2.0$	MEDIUM $2.0 \times 2.0 = 4.0$	MEDIUM $2.0 \times 3.0 = 6.0$	MEDIUM $2.0 \times 4.0 = 8.0$	HIGH $2.0 \times 5.0 = 10.0$
	POSSIBLE (3.0)	LOW $3.0 \times 1.0 = 3.0$	MEDIUM $3.0 \times 2.0 = 6.0$	MEDIUM $3.0 \times 3.0 = 9.0$	HIGH $3.0 \times 4.0 = 12.0$	HIGH $3.0 \times 5.0 = 15.0$

	<b>LIKELY</b>  <b>(4.0)</b>	<b>MEDIUM</b>  $4.0 \times 1.0 = 4.0$	<b>MEDIUM</b>  $4.0 \times 2.0 = 8.0$	<b>HIGH</b>  $4.0 \times 3.0 = 12.0$	<b>HIGH</b>  $4.0 \times 4.0 = 16.0$	<b>CRITICAL</b>  $4.0 \times 5.0 = 20.0$
	<b>CERTAIN</b>  <b>(5.0)</b>	<b>MEDIUM</b>  $5.0 \times 1.0 = 5.0$	<b>HIGH</b>  $5.0 \times 2.0 = 10.0$	<b>HIGH</b>  $5.0 \times 3.0 = 15.0$	<b>CRITICAL</b>  $5.0 \times 4.0 = 20.0$	<b>CRITICAL</b>  $5.0 \times 5.0 = 25.0$

## Risk Remediation

- As part of this risk remediation process, the Company shall determine objectives for mitigating or treating risks. All high and critical risks must be treated. For continuous improvement purposes, company managers may also opt to treat medium and/or low risks for company assets.
- Treatment options for risks include the following options:
  - Selection or development of security control(s).
  - Transferring the risks to a third party; for example, by purchasing an insurance policy or signing a contract with suppliers or partners.
  - Avoiding the risk by discontinuing the business activity that causes such risk.
  - Accepting the risk; this option is permitted only if the selection of other risk treatment options would cost more than the potential impact of the risk being realized.
- After selecting a treatment option, the risk owner should estimate the new impact and likelihood values after the planned controls are implemented.

## Regular Reviews of Risk Assessment and Risk Treatment

- The Risk Assessment Report must be updated when newly identified risks are identified. At a minimum, this update and review shall be conducted **once per year**.

## Reporting

- The results of risk assessments, and all subsequent reviews, shall be documented in a Risk Assessment Report.

## Change Log

Version	Date	Author	Summary
---------	------	--------	---------

1.0	2021-06-23	Kyle Randolph	Responded to Governance Committee feedback
0.1	2021-06-11	Kyle Randolph	Initial draft

Driven Security  
adam@drivenlocks.com

Verkada Inc.



# Verkada

Command Platform

## System and Organization Controls (SOC) 2 Type 2 Report

Report on Verkada Inc.'s Description of its Command Platform System and on the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security

Throughout the Period April 1, 2024 to September 30, 2024



## Table of Contents

I. INDEPENDENT SERVICE AUDITOR’S REPORT .....	3
II. ASSERTION OF VERKADA MANAGEMENT.....	8
III. VERKADA’S DESCRIPTION OF ITS COMMAND PLATFORM SYSTEM.....	11
Scope and Boundaries of the System.....	12
Components of the System Used to Provide the Services .....	14
Description of the Controls Relevant to the Applicable Criteria .....	21
Complementary Subservice Organization Controls.....	26
Complementary User Entity Controls.....	28
User Entity Responsibilities .....	28
IV. TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, TESTS OF CONTROLS, AND RESULTS OF TESTS.....	29
V. OTHER INFORMATION PROVIDED BY VERKADA THAT IS NOT COVERED BY THE SERVICE AUDITOR’S REPORT .....	106

## I. Independent Service Auditor's Report

## Independent Service Auditor's Report

To the Management of Verkada Inc.

### Scope

We have examined Verkada Inc.'s (Verkada) accompanying description of its Command Platform system found in Section III titled "Verkada's Description of its Command Platform System" throughout the period April 1, 2024 to September 30, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2024 to September 30, 2024, to provide reasonable assurance that Verkada's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Verkada uses Amazon Web Services (AWS), a subservice organization, to provide cloud infrastructure services; Backblaze, a subservice organization, to provide cloud data storage services; Okta, a subservice organization, to provide identity and access management services; and GitHub, a subservice organization, to provide code management and continuous integration services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Verkada to achieve Verkada's service commitments and system requirements based on the applicable trust services criteria. The description presents Verkada's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Verkada's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Verkada, to achieve Verkada's service commitments and system requirements based on the applicable trust services criteria. The description presents Verkada's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Verkada's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section V, "Other Information Provided by Verkada That is Not Covered by the Service Auditor's Report," is presented by Verkada's management to provide additional information and is not a part of Verkada's description of its Command Platform system made available to user entities during the period April 1, 2024 to September 30, 2024. Information about Verkada's response to the exception has not been subjected to the procedures applied in the examination and accordingly, we express no opinion on it.

### Service Organization's Responsibilities

Verkada is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Verkada's service commitments and system requirements were achieved. In Section II,

Verkada has provided the accompanying assertion titled “Assertion of Verkada Management” (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Verkada is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

### **Service Auditor’s Responsibilities**

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves—

- obtaining an understanding of the system and the service organization’s service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

### **Inherent Limitations**

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the

suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

### Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests are listed in Section IV, "Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests" of this report.

### Basis for Qualified Opinion

The accompanying description of Verkada's Command Platform system states that Verkada reviews compliance reports for high-risk vendors annually. However, for three out of seven high-risk vendors selected for testing, the review of compliance reports was not documented and for four out of seven high-risk vendors selected for testing, the review of compliance reports was not complete and accurate. As a result, the controls were not operating effectively throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion *CC9.2 - The entity assesses and manages risks associated with vendors and business partners.*

### Opinion

In our opinion, in all material respects—

- a) The description presents Verkada's Command Platform system that was designed and implemented throughout the period April 1, 2024 to September 30, 2024 in accordance with the description criteria.
- b) The controls stated in the description were suitably designed throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that Verkada's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Verkada's controls throughout that period.
- c) Except for the matter described in the Basis for Qualified Opinion paragraph, the controls stated in the description operated effectively throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that Verkada's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Verkada's controls operated effectively throughout that period.

### Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of Verkada; user entities of Verkada's Command Platform system during some or all of the period April 1, 2024 to September 30, 2024; business partners of Verkada subject to risks arising from interactions with the Command Platform system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.

- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

*Geels Norton LLC*

Geels Norton LLC  
Durham, North Carolina  
December 9, 2024

## II. Assertion of Verkada Management

## Assertion of Verkada Management

We have prepared the accompanying description of Verkada Inc.'s (Verkada) Command Platform system titled "Verkada's Description of its Command Platform System" throughout the period April 1, 2024 to September 30, 2024 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the Command Platform system that may be useful when assessing the risks arising from interactions with Verkada's system, particularly information about system controls that Verkada has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Verkada uses Amazon Web Services (AWS), a subservice organization, to provide cloud infrastructure services; Backblaze, a subservice organization, to provide cloud data storage services; Okta, a subservice organization, to provide identity and access management services; and GitHub, a subservice organization, to provide code management and continuous integration services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Verkada, to achieve Verkada's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the service organization's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Verkada, to achieve Verkada's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that—

1. The description presents Verkada's Command Platform system that was designed and implemented throughout the period April 1, 2024 to September 30, 2024 in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that Verkada's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Verkada's controls throughout that period.
3. Except for the matter described in paragraph 4, the controls stated in the description operated effectively throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that Verkada's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls



and complementary user entity controls assumed in the design of Verkada's controls operated effectively throughout that period.

- 4) The accompanying description of Verkada's Command Platform system states that Verkada reviews compliance reports for high-risk vendors annually. for three out of seven high-risk vendors selected for testing, the review of compliance reports was not documented and for four out of seven high-risk vendors selected for testing, the review of compliance reports was not complete and accurate. As a result, the controls were not operating effectively throughout the period April 1, 2024 to September 30, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on trust services criterion *CC9.2 - The entity assesses and manages risks associated with vendors and business partners.*

Verkada Management

### III. Verkada's Description of its Command Platform System

## Scope and Boundaries of the System

This is a System and Organization Controls (SOC) 2 Type 2 report and includes a description of Verkada Inc.'s (Verkada, service organization, or Company) Command Platform system, and the controls in place to provide reasonable assurance that Verkada's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), throughout the period April 1, 2024 to September 30, 2024, which may be relevant to users of the Command Platform system. It does not encompass all aspects of the services provided or procedures followed for other activities performed by Verkada.

### Company Background and Services Provided

Verkada was founded in 2016. Headquartered in San Mateo, California, Verkada provides its customers with cloud-managed physical security devices, including cameras, environmental sensors, camera viewing stations, access control devices, and intrusion detection devices, and a cloud-managed visitor management system. These devices and the visitor management system are managed through Verkada's cloud-based Command Platform, which is used by customers to protect people and assets, secure facilities, and gain new insights that improve the efficiency of their physical security operations.

The system description in this report details the Command Platform. Management and maintenance of the security of physical security devices, such as cameras and sensors, connected to the Command Platform or any other services offered by Verkada were not considered to be in scope for purposes of this report.

In September 2023, Verkada launched a new production cloud infrastructure account to support the servicing of EU-based customers and in April 2024 Verkada launched a new production cloud infrastructure account to support the servicing of Australia-based customers. The US, EU and Australia production accounts were considered to be in scope for the purposes of this report.

### Subservice Providers

Verkada uses AWS to provide cloud infrastructure services, Backblaze to provide cloud data storage services, Okta to provide identity and access management services, and GitHub to provide code management and continuous integration services. The description presents Verkada's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Verkada's controls. The description does not disclose the actual controls at the subservice organizations.

### Principal Service Commitments and System Requirements

Verkada designs its processes and procedures to meet objectives for its Command Platform system. Those objectives are based on the service commitments that Verkada makes to user entities and the system requirements that Verkada has established for their services.

Security commitments are standardized and include implementing commercially reasonable technical, administrative, and organizational measures to protect customer data from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. Additional commitments include, but are not limited to the following:

- Authorizing access to information resources, including production systems and customer data, on the principle of least privilege and conducts annual access control reviews

- Requiring two factor authentication and/or single sign-on to access sensitive systems and applications
- Establishing formal guidelines for employee passwords to govern the management and use of authentication mechanisms, and requiring the use of password managers, automatic screensaver locks, hard disk encryption, and other endpoint security measures
- Implementing a version control system helps manage source code, documentation, release labeling, and other change management tasks
- Implementing business continuity and incident response plans to effectively respond to a business interruption or security incident to minimize impact to customers
- Implementing formal risk management processes specify risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances. Verkada conducts a risk assessment at least annually
- Performing regular backups and retains them in accordance with a predefined schedule
- Ensuring that all connections to its web application from its users are encrypted using certificated TLS configurations
- Storing customer data in databases that are encrypted at rest
- Using configurations that ensure only approved networking ports and protocols are implemented
- Monitoring server CPU use, free storage space, message age and read I/O in Verkada's databases, servers and messaging queues and notify appropriate personnel of any events or incidents based on predetermined criteria

Verkada establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Verkada's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how internal networks are managed, and how employees are hired and trained.

### **System Incidents**

Verkada did not identify any system incidents that occurred during the period April 1, 2024 to September 30, 2024 that were the result of controls that were not suitably designed or operating effectively, or that resulted in a significant failure in the achievement of one or more of the service commitments or system requirements.

### **Significant Changes to the System and Controls**

Verkada did not identify any significant changes to the system or controls during the examination period.

## Components of the System Used to Provide the Services

### Infrastructure

Verkada supports a remote workforce. Verkada issues company workstations to new employees upon hire and provisions access to Verkada systems, which operates on software as a service (SaaS) platforms.

Verkada's Command Platform web-based platform ("the platform") is maintained on an AWS cloud environment. The following are key infrastructure services used by the platform:

Component	Purpose
AWS Route 53	Route 53 is a highly available and scalable Domain Name System (DNS) web service.
AWS CloudFront	CloudFront is a content delivery network (CDN) operated by AWS that provides a globally distributed network of proxy servers that cache content, more locally to consumers, to improve access speed for downloading the content.
AWS ELB	AWS Elastic Load Balancing (ELB) helps Verkada automatically distribute incoming application traffic across multiple targets and virtual appliances across multiple Availability Zones (AZs).
AWS VPC	AWS Virtual Private Cloud (VPC) is a service that lets Verkada launch AWS resources in logically isolated virtual networks that they define, including the provisioning of private subnets for production compute and database services.
AWS IAM	AWS Identity and Access Management (IAM) manages AWS users and groups using permission-based logical access management to allow and deny access to AWS resources.
AWS EC2	AWS Elastic Compute Cloud (EC2) is a virtual server service providing elastic compute cloud for running EKS.
AWS EKS	AWS Elastic Kubernetes Service (EKS) is an Amazon-managed service that Verkada uses to run Kubernetes on AWS.
AWS Lambda	An event-driven, serverless computing platform that runs code in response to events and automatically manages the computing resources required by that code.
AWS ElastiCache	ElastiCache is a fully managed in-memory data store and caching service that improves the performance of web applications by

Component	Purpose
	retrieving information from managed in-memory caches. Data such as customer's name, email address, physical address, etc. is stored here.
AWS RDS	AWS Relational Database Service (RDS) is a fully managed, open-source cloud database service that allows Verkada to easily operate and scale their databases used to support the Command Platform. RDS is used to store application service data such as user data, customer organizational data, and customer device information.
AWS DynamoDB	DynamoDB is a fully managed proprietary NoSQL database service that supports key-value and document data structures and offers continuous backups, automated multi-region replication, and in-memory caching. DynamoDB stores customer user and product metadata.
AWS S3	AWS Simple Storage Service (S3) is an object storage service offering industry-leading scalability, data availability, security, and performance. Verkada uses S3 buckets to store video footage from Verkada's customers' cameras, as well as infrastructure log files.
Backblaze	Backblaze is used by Verkada as the primary cloud data storage service to store encrypted backups of video footage from Verkada's customers' cameras. Backblaze is Verkada's default storage service for the storage of customer video files unless customers specifically request the use of AWS S3 in scenarios, such as geographic limitations, where Backblaze is not available.

## Software

Verkada uses the following software in support of the platform and related business processes:

Software	Purpose
Okta	Okta is an identity and access management service used by Verkada to manage and secure user authentication into applications.
GitHub	GitHub is the source code repository and continuous integration (CI) platform used by Verkada.

Software	Purpose
Terraform	Infrastructure as code software tool to manage cloud services and configurations.
MonoCI	Verkada's in-house developed tool to facilitate the execution of continuous integration tests for specific production services.
Bazel	Verkada uses Bazel to facilitate the execution of continuous integration tests and the building of new containers for deployment to production for specific production services.
Argo CD	Verkada uses Argo CD to support the continuous deployment (CD) of code to the platform.
AWS CodeBuild	Verkada uses CodeBuild in conjunction with code that is tested through MonoCI to support the building and packaging of new code for deployment.
Datadog	Observability service for cloud-scale applications, providing performance monitoring for servers, databases, tools, and services, through a SaaS-based data analytics platform.
OpenSearch	Verkada uses OpenSearch for device logging and monitoring alongside Datadog. OpenSearch is used to monitor Verkada customer Internet of Things (IoT) devices connected to the Command Platform. Verkada self-hosts OpenSearch within their own AWS environment. Data such as customer's name, email address, physical address, etc. is stored here. No customer data processed through the Command Platform is stored here.
Orca Security	Orca Security is agentless, workload-deep, context-aware cloud infrastructure security and compliance service used to monitor activity for Verkada's infrastructure, including infrastructure vulnerabilities and potential non-compliance with industry security benchmarks. Verkada also uses Orca's File Integrity Monitoring (FIM) service.
Wiz	Wiz is a cloud security tool used by Verkada that provides visibility into cloud infrastructure, identifying security risks, vulnerabilities, and compliance issues across cloud environments. <i>Verkada began using Wiz on August 5, 2024.</i>

Software	Purpose
Panther	<p>Panther is a cloud-based security information and event management (SIEM) tool used by Verkada to aggregate logs and configure security alerts, including intrusion detection.</p> <p><i>Verkada deprecated Panther on September 7, 2024.</i></p>
vStreamAlert	<p>An in-house developed tool used by Verkada to aggregate logs and configure security alerts, including intrusion detection.</p> <p><i>Verkada began using vStreamAlert on August 31, 2024.</i></p>
OpsGenie	<p>OpsGenie is an incident response tool used by Verkada which has been configured to receive critical performance alerts, notify the appropriate teams, and to log events through resolution.</p>
Google Maps API	<p>Verkada's visitor management module of the Command Platform uses the Google Maps API to resolve visitor's addresses. Visitor data is not stored in Google's cloud environment.</p>
Drata	<p>Drata is the compliance automation tool used by Verkada to track and manage their compliance with company security requirements.</p>
Kandji	<p>Kandji is a mobile device management (MDM) platform for Mac devices.</p>
JumpCloud	<p>JumpCloud is an MDM platform for Windows and Linux devices.</p>
Linear	<p>Linear helps Verkada plan, assign, track, report, and manage work as a ticketing and work management tool.</p>
Twilio	<p>Communications tool used by Verkada to send product and service-related updates and alerts to customers.</p>
Intercom	<p>Verkada uses Intercom for live chat support for customers when they are using the Command Platform.</p>
BambooHR	<p>BambooHR is the human resources information system (HRIS) used by Verkada to manage and maintain onboarding and compliance requirements for their employees.</p>



Software	Purpose
Lattice	Verkada uses Lattice as their people management platform to conduct their employee performance management program.
Checkr	Verkada uses Chekr as their background check service provider for new hires.
Salesforce	Verkada uses Salesforce as a customer relationship management tool.

## People

Verkada is organized by functional area. Within functional areas, organizational and reporting hierarchies are defined and responsibilities are assigned.

Component	Responsibilities
Executive Leadership Team (ELT)	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Security and Privacy Governance Committee	Responsible for overseeing performance of the security and privacy programs, risk management, and strategy.
People (Human Resources)	Responsible for onboarding new personnel, assigning the roles and positions of new hires, maintaining the Employee Handbook and its acceptance by personnel, performing background checks, maintaining organization charts, and facilitating the employee termination process.
Legal	Responsible for advising on legal and regulatory issues related to security and privacy
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Engineering	Responsible for the development, testing, deployment, and maintenance of source code for the Command Platform. Assists customers with technical support when necessary.
Information Technology (IT)	Responsible for managing corporate IT infrastructure, including corporate IT security controls and laptops issued to Company personnel.
Security	Responsible for defining and executing the Company's security and compliance activities, and managing access to the engineering infrastructure.
Support	Responsible for providing technical support to customers.

## **Policies and Procedures**

Verkada maintains the following documented policies and procedures to support the internal control environment:

- Acceptable Use Policy
- Acceptable Use of Products Policy
- Acceptable Use of Technology Policy
- Access Control Policy
- Asset Management Policy
- Background Check Standard
- Business Continuity Plan
- Change Management Standard
- Data Classification Policy
- Data Protection Policy
- Data Retention Standard
- Disaster Recovery Plan
- Employee Handbook
- Eng Access Management Standard
- Generative AI Policy
- Incident Response Plan
- Information Security Policy
- Network Security Standard
- Password Policy
- Physical Security Policy
- Remote Access Standard
- Risk Management Policy
- Secrets Management Standard
- Secure Communications Standard
- Security and Privacy Governance Committee
- Security Vulnerability Management Standard
- Software and Open Source Policy
- System Hardening Standard
- System Security Monitoring Standard
- Vendor Risk and Compliance Management Policy

## **Data**

Data stored and processed by the Command Platform system consists of customer data such as names, contact information, images, video recordings, and application usage data, along with application and infrastructure logs.

Data is classified by risk and controls are applied based on the classification. Data retention and data destruction policies and procedures are in place and employees are trained on the proper use and safeguards of data.

## Description of the Controls Relevant to the Applicable Criteria

Verkada has specified the scope of this examination to include the Security category and has identified the controls that have been designed and operated to achieve the related trust services criteria based on Verkada's service commitments and system requirements. Verkada's controls are presented below.

### Control Environment

#### Organizational Governance and Structure

- Verkada maintains an organizational chart which includes organizational structure, reporting lines, and authorities.
- Members of the Board of Directors are independent of management.
- The Board of Directors meets quarterly to provide oversight and guidance to Verkada management, including organizational, internal control, and information security risk management strategies.
- The Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations. The Committee members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.

#### Roles and Responsibilities

- Management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.
- Verkada positions have detailed job descriptions that list qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Verkada.

#### Hiring and Onboarding

- Verkada's new hires are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their specific job responsibilities.
- Verkada new hires are required to pass a background check as a condition of their employment.
- Verkada's Employee Handbook includes a formal Code of Conduct which is approved by management and accessible to all employees. Employees must sign the Employee Handbook upon hire.
- Verkada has policies and procedures in place to establish acceptable use of information assets approved by management. Employees must sign the Acceptable Use Policy upon hire.

#### Employee Training and Development

- Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.
- Verkada evaluates the performance of employees through annual performance evaluations.

## **Communication and Information**

### **Policies and Procedures**

- Verkada Management has approved security policies, and all employees accept these procedures when hired.
- Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.
- Verkada has an established policy and procedures that govern the use of cryptographic controls.

### **Internal Communications**

- Verkada provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, along with any other complaints to the company management.
- The Security team communicates important information security events to company management in a timely manner.
- Verkada maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.

### **External Communications**

- Verkada maintains an End User Agreement that is available to all external users and that details the company's security commitments regarding the systems. External users must accept the End User Agreement prior to their account being created on Verkada's Command Platform.
- Verkada communicates system changes to customers that may affect security and availability.
- Verkada provides a process to customers and external users for reporting security failures, incidents, and concerns.

## **Risk Assessment**

- Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.
- Verkada conducts a formal risk assessment which is reviewed at least annually.
- Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

## **Monitoring Activities**

### **Internal Control Monitoring**

- Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.
- Verkada uses a cloud-based system and control monitoring tool to help monitor control activities and ensure internal controls are operating as anticipated. The Security Engineering Team meets on a weekly basis to review failing controls presented in the monitoring tools' dashboard.
- Verkada performs control self-assessments at least annually to gain assurance that security controls are in place and operating effectively. Corrective actions are taken based on relevant findings.

### Penetration Testing and 3rd Party Assessments

- Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.
- Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and critical and high-priority findings are tracked to resolution.

### Logical Access Controls

#### User Access Management

- Verkada uses role-based access through Okta to provision access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.
- Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles.
- Verkada restricts administrative access to AWS, Backblaze, GitHub, the Command Platform, Cloudflare, and Twilio to authorized personnel based on job requirements.
- Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.
- Verkada's Command Platform user passwords are stored using a salted password hash.
- System access is removed from terminated employees within one business day. Employee devices are locked as part of the offboarding process.
- Verkada performs user access control reviews for AWS, Backblaze, GitHub, Argo CD, and the Command Platform annually, at minimum.

#### Data Storage and Encryption

- Read/write access to S3 buckets and Backblaze is configured to restrict public access.
- Data stored in S3 buckets, RDS databases, and Backblaze databases is encrypted at rest.

#### Data Retention and Disposal

- Verkada has a Data Deletion Policy to help guide the deletion of customer data.

#### Perimeter Security

- Verkada configures security groups and load balancers to restrict access to production environment resources to authorized traffic.
- Verkada configures network access control lists (NACLs) at the subnet level to help restrict access to authorized traffic.
- An intrusion detection system (IDS) is in place to detect potential intrusions and alert personnel when a potential intrusion is detected.

#### Transmission of Information

- Verkada enforces secure and encrypted connections when accessing production and staging resources.
- Verkada ensures that all connections to its web application from its users are encrypted.
- Verkada enforces secure transmission of information when sending data to the cloud storage provider.

### Workstation Security

- MDM systems are in place to centrally manage mobile devices supporting the service.
- Verkada ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.
- Verkada ensures that company-issued laptops have encrypted hard-disks.
- Verkada's workstation operating system security patches are applied automatically.
- Verkada requires antivirus software to be installed on workstations to protect the network against malware.

### System Operations

#### Security Monitoring

- Verkada has enabled infrastructure logs throughout their production environment. Infrastructure logs are stored encrypted, log file validation is enabled, and access to infrastructure logs is restricted to those who require access to perform their job duties.
- Verkada has configured SIEM tools that collect and store server logs in a central location. Access to the logs stored in the SIEM tools is restricted to authorized users.
- Verkada has configured its SIEM tools to send alerts to the business communications channel to alert the appropriate teams when anomalous system events occur. The SIEM tools are also configured to automatically create a ticket in their issue and project tracking software when critical and high-severity events occur, where the events are logged and tracked through resolution.
- Verkada ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.

#### Performance Monitoring

- Verkada has configured a cloud observability service to monitor their cloud infrastructure for system performance issues. Critical and high-severity alerts are sent to the incident response tool to alert the on-call engineer.

#### Incident Response

- Verkada has an established Cybersecurity Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.
- Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.
- Security incidents are logged, tracked, resolved, and communicated to affected parties by management according to Verkada's security incident response policies and procedures. All security incidents are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.
- Verkada has implemented a Cybersecurity Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.
- Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.
- Verkada ensures that incident response plan testing is performed on an annual basis.



## **Change Management**

- Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.
- Separate environments are used for testing and production for Verkada's application.
- Verkada's customer data is segregated from the data of other customers.
- Verkada uses a version control system to manage source code, documentation, release labeling, and other change management tasks.
- Verkada ensures that code changes are tested prior to implementation to ensure quality and security.
- Verkada systematically requires code changes to undergo code reviews and tests prior to merging to the master branch by someone other than the person who made the code change.
- Verkada ensures that releases are approved by code owners prior to merging into the master branch.
- Verkada restricts deployment permissions to engineers through role-based access.
- Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.
- Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days. Tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.

## **Risk Mitigation**

### **Data Backup and Restoration**

- Verkada performs database backups daily and retains them in accordance with a predefined schedule in the Backup Policy.

### **Disaster Recovery and Business Continuity**

- Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.
- Verkada conducts annual disaster recovery tests and documents results according to the Disaster Recovery Plan.
- Verkada maintains cybersecurity insurance to mitigate the financial impact of business disruptions.

### **Vendor Management**

- Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.
- Verkada maintains a directory of its key vendors, including their compliance reports. High-risk vendor compliance reports are reviewed annually.
- Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.



## Complementary Subservice Organization Controls

Verkada's controls related to the Command Platform system cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Verkada's controls. The complementary subservice organization controls in the table below are expected to be implemented and operating effectively:

Number	Complementary Subservice Organization Control ("CSOC")	Applicable Criteria
AWS		
1.	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1, CC6.3
2.	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	CC6.4
3.	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.	CC6.5
4.	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC3.2, CC3.4, CC9.1
5.	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CC7.5, CC9.1
6.	The entity designs and maintains system infrastructure for high availability and tests recovery plan procedures supporting system recovery to meet its objectives.	CC6.7, CC,9.1
7.	The entity restricts access to data and software to personnel authorized and provisioned with logical security controls.	CC6.1, CC6.2, CC6.3
8.	The entity designs, develops, and maintains software to transmit confidential data securely, and ensures that connections over public networks between trusted parties are encrypted.	CC6.7
9.	The entity practices secure software change and development procedures to help prevent against vulnerabilities.	CC8.1
10.	The entity designs, maintains and monitors the security of operating systems supporting managed compute and data storage services.	CC6.8, CC7.1, CC7.2, CC7.3
11.	The entity encrypts and backs up DynamoDB databases where customer data resides.	CC6.1, CC6.6, CC9.1

Number	Complementary Subservice Organization Control ("CSOC")	Applicable Criteria
GitHub, Okta, Backblaze		
1.	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	CC6.1, CC6.3
2.	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC3.2, CC3.4, CC9.1
3.	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	CC7.5, CC9.1
4.	The entity designs and maintains system infrastructure for high availability and tests recovery plan procedures supporting system recovery to meet its objectives.	CC6.7, CC9.1
5.	The entity restricts access to data and software to personnel authorized and provisioned with logical security controls.	CC6.1, CC6.2, CC6.3
6.	The entity designs, develops, and maintains software to transmit confidential data securely, and ensures that connections over public networks between trusted parties are encrypted.	CC6.7
7.	The entity practices secure software change and development procedures to help prevent against vulnerabilities.	CC8.1

## Complementary User Entity Controls

Verkada's controls related to the Command Platform system cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Verkada's controls. The complementary user entity controls in the table below are expected to be implemented and operating effectively:

Number	Complementary User Entity Control	Applicable Criteria
1.	Reporting issues or security concerns related to the Command Platform system to Verkada Inc. in a timely manner.	CC2.3, CC3.3

## User Entity Responsibilities

Verkada's system is designed with the assumption that certain responsibilities fall to the user of the system. The control responsibilities listed below are the responsibility of the users of the system. These controls are expected to be in operation at the user entities to complement Verkada's controls. User entities are responsible for their own control environments and their operational effectiveness. The list of controls below should not be a comprehensive list of all control activities that should be implemented by user entities.

Number	User Entity Responsibility
1.	Cooperating with Verkada in establishing account credentials for verifying that only designated employees have access to administrative functions of the Command Platform system.
2.	Protecting the security of customer account credentials for access to Verkada systems that store or process confidential data.
3.	Performing periodic reviews of user access to customer's account.
4.	Complying with applicable contracts and Verkada's terms of service, including the use of reasonable efforts to prevent unauthorized access to or use of the Platform, and immediate notification to Verkada of unauthorized access and use of the Command Platform system.
5.	Transmitting documents containing sensitive information via encrypted data connections approved by Verkada .

#### IV. Trust Services Categories, Criteria, Related Controls, Tests of Controls, and Results of Tests

## Information Provided by the Service Auditor

This report is intended to provide information to the management of Verkada, user entities of the Verkada's Command Platform system, and prospective user entities, independent auditors and practitioners providing services to those entities, who have a sufficient understanding to consider it, along with other information including information about the controls implemented by the user entity. This report is intended to provide information about the suitability of the design and operating effectiveness of the controls implemented to achieve the service commitments and system requirements based on the criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), throughout the period April 1, 2024 to September 30, 2024.

Although the applicable trust services criteria and related controls are presented in this section, they are an integral part of Verkada's description of its Command Platform system throughout the period April 1, 2024 to September 30, 2024.

The examination was performed in accordance with attestation standards established by the American Institute of Certified Public Accountants, specifically AT-C sections 105 and 205 and the guidance contained in the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. It is each user entity's responsibility to evaluate this information in relation to the internal control structure in place at each user entity in order to assess the total internal control structure. If an effective internal control structure is not in place at user entities, Verkada's controls may not compensate for such weaknesses.

This description is intended to focus on Verkada's controls surrounding the Command Platform system throughout the period April 1, 2024 to September 30, 2024; it does not encompass all aspects of the services provided or controls performed by Verkada. Unique processes or control situations not described in the report are outside the scope of this report.

### Tests of Controls

Our examination of the description of Verkada's Command Platform system and the suitability of the design and operating effectiveness of the controls to achieve the related service commitments and system requirements based on the services criteria stated in the description involved performing procedures to obtain evidence about the presentation of the description of the system in accordance with the description criteria and the suitability of the design and operating effectiveness of those controls to achieve the related service commitments and system requirements based on the services criteria stated in the description. Our procedures included assessing the risks that the description is not presented in accordance with the description criteria and that the controls were not suitably designed or operating effectively to achieve the related service commitments and system requirements based on the services stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related service commitments and system requirements based on the applicable trust services criteria stated in the description were achieved throughout the period April 1, 2024 to September 30, 2024.

Our tests of controls were designed to cover a representative number of activities throughout the April 1, 2024 to September 30, 2024, for each of the controls listed in Section IV, which are designed to achieve the related service commitments and system requirements based on the

applicable trust services criteria. In selecting particular tests of controls, we considered: (a) the nature of the controls being tested, (b) the types and competence of available evidential matter, (c) the criteria to be achieved, (d) the assessed level of control risk, and (e) the expected efficiency and effectiveness of the test.

Geels Norton LLC's testing of controls was restricted to the controls specified by Verkada in Section IV, and was not extended to controls in effect at user locations or other controls which were not documented as tested under each control criteria listed in Section IV. The description of Geels Norton LLC's tests of controls and results of those tests are presented in this section of the report. The description of the tests of controls and the results of those tests are the responsibility of Geels Norton LLC and should be considered information provided by Geels Norton LLC.

## CC1.0 - Common Criteria Related to the Control Environment

CC1.1 - The entity demonstrates a commitment to integrity and ethical values.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.1.1	Members of the Board of Directors are independent of management.	Inspected the list of Board of Directors to determine that members of the Board of Directors are independent of management.	No exceptions noted.
CC1.1.2	The Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations. The Committee members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	<p>Inspected the Security and Privacy Committee Charter to determine that the Committee members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.</p> <p>Inspected the meeting agenda and related action items from a Security and Privacy Governance Committee meeting during the examination period to determine that the Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations.</p>	No exceptions noted.
CC1.1.3	Verkada new hires are required to pass a background check as a condition of their employment.	Inspected the background checks for a selection of US-based new employees to determine that Verkada new hires are required to pass a background check as a condition of their employment.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.1.4	Verkada's Employee Handbook includes a formal Code of Conduct which is approved by management and accessible to all employees. Employees must sign the Employee Handbook upon hire.	Inspected the Employee Handbook and the signed Employee Handbook for a selection of new employees to determine that Verkada's Employee Handbook includes a formal Code of Conduct, which is approved by management and accessible to all employees, and that employees must sign the Employee Handbook upon hire.	No exceptions noted.



CC1.2 - The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.2.1	Members of the Board of Directors are independent of management.	Inspected the list of Board of Directors to determine that members of the Board of Directors are independent of management.	No exceptions noted.
CC1.2.2	Management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.	No exceptions noted.
CC1.2.3	Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Security and Privacy Governance Committee Charter, the meeting agenda from a Committee meeting during the examination period, and Committee action items to determine that Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.
CC1.2.4	The Security team communicates important information security events to company management in a timely manner.	Inspected the Security team's recurring meeting invites and the presentation deck from a meeting during the examination period to determine that the Security team communicates important information security events to company management in a timely manner.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.2.5	The Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations. The Committee members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	<p>Inspected the Security and Privacy Committee Charter to determine that the Committee members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.</p> <p>Inspected the meeting agenda and related action items from a Security and Privacy Governance Committee meeting during the examination period to determine that the Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations.</p>	No exceptions noted.
CC1.2.6	The Board of Directors meets quarterly to provide oversight and guidance to Verkada management, including organizational, internal control, and information security risk management strategies.	Inspected the board presentation for a sample of quarters to determine that the Board of Directors meets quarterly to provide oversight and guidance to Verkada management, including organizational, internal control, and information security risk management strategies.	No exceptions noted.

CC1.3 - Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.3.1	Verkada maintains an organizational chart which includes organizational structure, reporting lines, and authorities.	Inspected the organizational chart to determine that Verkada maintains an organizational chart which includes organizational structure, reporting lines, and authorities.	No exceptions noted.
CC1.3.2	Verkada positions have detailed job descriptions that list qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Verkada.	Inspected the job descriptions for a selection of new employees to determine that Verkada positions have detailed job descriptions that list qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Verkada.	No exceptions noted.
CC1.3.3	Management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.	No exceptions noted.
CC1.3.4	Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Security and Privacy Governance Committee Charter, the meeting agenda from a Committee meeting during the examination period, and Committee action items to determine that Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.3.5	The Security team communicates important information security events to company management in a timely manner.	Inspected the Security team's recurring meeting invites and the presentation deck from a meeting during the examination period to determine that the Security team communicates important information security events to company management in a timely manner.	No exceptions noted.

CC1.4 - The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.4.1	Verkada's new hires are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their specific job responsibilities.	Inspected evidence of interview evaluations for a selection of new employees to determine that Verkada's new hires are required to go through an official recruiting process during which their qualifications and experience are screened to ensure that they are competent and capable of fulfilling their specific job responsibilities.	No exceptions noted.
CC1.4.2	Verkada positions have detailed job descriptions that list qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Verkada.	Inspected the job descriptions for a selection of new employees to determine that Verkada positions have detailed job descriptions that list qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by Verkada.	No exceptions noted.
CC1.4.3	Verkada new hires are required to pass a background check as a condition of their employment.	Inspected the background checks for a selection of US-based new employees to determine that Verkada new hires are required to pass a background check as a condition of their employment.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.4.4	Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the completed information security training for a selection of new employees and existing employees to determine that Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents, and that full-time employees are required to complete the training upon hire.	No exceptions noted.
CC1.4.5	Verkada evaluates the performance of employees through annual performance evaluations.	Inspected the performance evaluations for a selection of employees employed for over one year to determine that Verkada performs annual performance evaluations for employees.	No exceptions noted.

CC1.5 - The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.5.1	Verkada's Employee Handbook includes a formal Code of Conduct which is approved by management and accessible to all employees. Employees must sign the Employee Handbook upon hire.	Inspected the Employee Handbook and the signed Employee Handbook for a selection of new employees to determine that Verkada's Employee Handbook includes a formal Code of Conduct, which is approved by management and accessible to all employees, and that employees must sign the Employee Handbook upon hire.	No exceptions noted.
CC1.5.2	Verkada has policies and procedures in place to establish acceptable use of information assets approved by management. Employees must sign the Acceptable Use Policy upon hire.	Inspected the Acceptable Use Policy to determine that Verkada has policies and procedures in place to establish acceptable use of information assets approved by management.  Inspected the signed Acceptable Use Policy for a selection of new employees to determine that employees must sign the Acceptable Use Policy upon hire.	No exceptions noted.
CC1.5.3	Verkada Management has approved security policies, and all employees accept these procedures when hired.	Inspected the security policy approval records to determine that Verkada Management has approved security policies.  Inspected the accepted security policies for a selection of new hires to determine that employees accept these procedures when hired.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC1.5.4	Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the completed information security training for a selection of new employees and existing employees to determine that Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents, and that full-time employees are required to complete the training upon hire.	No exceptions noted.
CC1.5.5	Verkada evaluates the performance of employees through annual performance evaluations.	Inspected the performance evaluations for a selection of employees employed for over one year to determine that Verkada performs annual performance evaluations for employees.	No exceptions noted.
CC1.5.6	The Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations. The Committee members have sufficient expertise to oversee management's ability to design, implement, and operate information security controls.	<p>Inspected the Security and Privacy Committee Charter to determine that the Committee members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.</p> <p>Inspected the meeting agenda and related action items from a Security and Privacy Governance Committee meeting during the examination period to determine that the Security and Privacy Governance Committee meets on a regular basis to review compliance with security and privacy practices and privacy regulations.</p>	No exceptions noted.



## CC2.0 - Common Criteria Related to Communication and Information

CC2.1 - The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Number	Description of Control	Description of Test	Result of Testing
CC2.1.1	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC2.1.2	Verkada performs control self-assessments at least annually to gain assurance that security controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the completed annual control assessment to determine that Verkada performs control self-assessments at least annually to gain assurance that security controls are in place and operating effectively, and that corrective actions are taken based on relevant findings.	No exceptions noted.
CC2.1.3	Verkada maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	Inspected the architecture diagrams to determine that Verkada maintains an accurate architecture diagram to document system boundaries to support the functioning of internal control.	No exceptions noted.
CC2.1.4	Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	Inspected the annual penetration test and retest report to determine that Verkada engages with a third-party to conduct penetration tests of the production environment at least annually, that results are reviewed by management, and that there were no critical and high-priority findings to track through resolution.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC2.1.5	Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	<p>Inspected the quarterly vulnerability scan results to determine that Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly.</p> <p>Inspected the quarterly vulnerability scan results to determine that there were no critical or high-priority findings to track to resolution.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to tracking critical and high-priority findings to resolution, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>
CC2.1.6	Verkada has configured its SIEM tools to send alerts to the business communications channel to alert the appropriate teams when anomalous system events occur. The SIEM tools are also configured to automatically create a ticket in their issue and project tracking software when critical and high-severity events occur, where the events are logged and tracked through resolution.	<p>Inspected the SIEM tools alerting configurations to determine that Verkada has configured its SIEM tools to send alerts to the business communications channel when anomalous system events occur and that a ticket is automatically created in their project tracking software when critical or high-severity events occur.</p> <p>Inspected the list of critical and high-severity issue tickets to determine that critical and high-severity security events are logged and tracked through resolution.</p>	No exceptions noted.

CC2.2 - The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control Number	Description of Control	Description of Test	Result of Testing
CC2.2.1	Verkada's Employee Handbook includes a formal Code of Conduct which is approved by management and accessible to all employees. Employees must sign the Employee Handbook upon hire.	Inspected the Employee Handbook and the signed Employee Handbook for a selection of new employees to determine that Verkada's Employee Handbook includes a formal Code of Conduct, which is approved by management and accessible to all employees, and that employees must sign the Employee Handbook upon hire.	No exceptions noted.
CC2.2.2	Verkada has policies and procedures in place to establish acceptable use of information assets approved by management. Employees must sign the Acceptable Use Policy upon hire.	Inspected the Acceptable Use Policy to determine that Verkada has policies and procedures in place to establish acceptable use of information assets approved by management.  Inspected the signed Acceptable Use Policy for a selection of new employees to determine that employees must sign the Acceptable Use Policy upon hire.	No exceptions noted.
CC2.2.3	Verkada Management has approved security policies, and all employees accept these procedures when hired.	Inspected the security policy approval records to determine that Verkada Management has approved security policies.  Inspected the accepted security policies for a selection of new hires to determine that employees accept these procedures when hired.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC2.2.4	Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents. Full-time employees are required to complete the training upon hire and annually thereafter.	Inspected the completed information security training for a selection of new employees and existing employees to determine that Verkada has established training programs for information security to help employees understand their obligations and responsibilities to comply with Verkada's security policies and procedures, including the identification and reporting of incidents, and that full-time employees are required to complete the training upon hire.	No exceptions noted.
CC2.2.5	Verkada provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, along with any other complaints to the company management.	<p>Inspected the Cybersecurity Incident Response Plan and training content from the most recent annual security training to determine that Verkada provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, along with any other complaints to the company management.</p> <p>Reperformed the submission of an email sent to Security@verkada.com to determine that Verkada maintains a Security@ email alias for employees to submit concerns, events, and issues to Verkada management for resolution.</p>	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC2.2.6	The Security team communicates important information security events to company management in a timely manner.	Inspected the Security team's recurring meeting invites and the presentation deck from a meeting during the examination period to determine that the Security team communicates important information security events to company management in a timely manner.	No exceptions noted.
CC2.2.7	The Board of Directors meets quarterly to provide oversight and guidance to Verkada management, including organizational, internal control, and information security risk management strategies.	Inspected the board presentation for a sample of quarters to determine that the Board of Directors meets quarterly to provide oversight and guidance to Verkada management, including organizational, internal control, and information security risk management strategies.	No exceptions noted.

CC2.3 - The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control Number	Description of Control	Description of Test	Result of Testing
CC2.3.1	Verkada maintains an End User Agreement that is available to all external users and that details the company's security commitments regarding the systems. External users must accept the End User Agreement prior to their account being created on Verkada's Command Platform.	<p>Inspected the End User Agreement on Verkada's website to determine that Verkada maintains an End User Agreement that is available to all external users and details the company's security commitments.</p> <p>Inspected the Verkada Command Platform profile creation page and login page to determine that external users must accept the End User Agreement prior to their account being created.</p>	No exceptions noted.
CC2.3.2	Verkada provides a process to customers and external users for reporting security failures, incidents, and concerns.	Inspected Verkada's vulnerability reporting form and vulnerability dashboard to determine that Verkada provides a process to customers and external users for reporting security failures, incidents, and concerns.	No exceptions noted.
CC2.3.3	Verkada communicates system changes to customers that may affect security and availability.	Inspected the Verkada product updates and status pages to determine that Verkada communicates system changes to customers that may affect security and availability.	No exceptions noted.
CC2.3.4	Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected Verkada's vendor directory and the terms of service for a selection of high-risk vendors to determine that Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted.

## CC3.0 - Common Criteria Related to Risk Assessment

CC3.1 - The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC3.1.1	Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Management Policy to determine that Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.1.2	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC3.1.3	Management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee implementation of information security policies across the organization.	No exceptions noted.
CC3.1.4	Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Security and Privacy Governance Committee Charter, the meeting agenda from a Committee meeting during the examination period, and Committee action items to determine that Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC3.1.5	Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	No exceptions noted.
CC3.1.6	Verkada uses a cloud-based system and control monitoring tool to help monitor control activities and ensure internal controls are operating as anticipated. The Security Engineering Team meets on a weekly basis to review failing controls presented in the monitoring tools' dashboard.	<p>Inspected the cloud-based system and control monitoring tool dashboard to determine that Verkada uses a cloud-based system and control monitoring tool to help monitor control activities and ensure internal controls are operating as anticipated.</p> <p>Inspected the recurring meeting invite and an example of the dashboard that is reviewed during the weekly meetings to determine that the Security Engineering Team meets on a weekly basis to review failing controls presented in the monitoring tools' dashboard.</p>	No exceptions noted.



CC3.2 - The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Control Number	Description of Control	Description of Test	Result of Testing
CC3.2.1	Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Management Policy to determine that Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.2.2	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC3.2.3	Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment and mitigation plans for remediation to determine that Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.

CC3.3 - The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC3.3.1	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC3.3.2	Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment and mitigation plans for remediation to determine that Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC3.3.3	Verkada new hires are required to pass a background check as a condition of their employment.	Inspected the background checks for a selection of US-based new employees to determine that Verkada new hires are required to pass a background check as a condition of their employment.	No exceptions noted.

CC3.4 - The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Number	Description of Control	Description of Test	Result of Testing
CC3.4.1	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC3.4.2	Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	Inspected the annual penetration test and retest report to determine that Verkada engages with a third-party to conduct penetration tests of the production environment at least annually, that results are reviewed by management, and that there were no critical and high-priority findings to track through resolution.	No exceptions noted.
CC3.4.3	Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	<p>Inspected the quarterly vulnerability scan results to determine that Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly.</p> <p>Inspected the quarterly vulnerability scan results to determine that there were no critical or high-priority findings to track to resolution.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to tracking critical and high-priority findings to resolution, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>

Control Number	Description of Control	Description of Test	Result of Testing
CC3.4.4	Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	Inspected the Vendor Risk and Compliance Management Policy to determine that Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	No exceptions noted.
CC3.4.5	The Security team communicates important information security events to company management in a timely manner.	Inspected the Security team's recurring meeting invites and the presentation deck from a meeting during the examination period to determine that the Security team communicates important information security events to company management in a timely manner.	No exceptions noted.

## CC4.0 - Common Criteria Related to Monitoring Activities

CC4.1 - The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control Number	Description of Control	Description of Test	Result of Testing
CC4.1.1	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC4.1.2	Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	Inspected the annual penetration test and retest report to determine that Verkada engages with a third-party to conduct penetration tests of the production environment at least annually, that results are reviewed by management, and that there were no critical and high-priority findings to track through resolution.	No exceptions noted.
CC4.1.3	Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	<p>Inspected the quarterly vulnerability scan results to determine that Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly.</p> <p>Inspected the quarterly vulnerability scan results to determine that there were no critical or high-priority findings to track to resolution.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to tracking critical and high-priority findings to resolution, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>

Control Number	Description of Control	Description of Test	Result of Testing
CC4.1.4	Verkada uses a cloud-based system and control monitoring tool to help monitor control activities and ensure internal controls are operating as anticipated. The Security Engineering Team meets on a weekly basis to review failing controls presented in the monitoring tools' dashboard.	<p>Inspected the cloud-based system and control monitoring tool dashboard to determine that Verkada uses a cloud-based system and control monitoring tool to help monitor control activities and ensure internal controls are operating as anticipated.</p> <p>Inspected the recurring meeting invite and an example of the dashboard that is reviewed during the weekly meetings to determine that the Security Engineering Team meets on a weekly basis to review failing controls presented in the monitoring tools' dashboard.</p>	No exceptions noted.
CC4.1.5	Verkada performs control self-assessments at least annually to gain assurance that security controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the completed annual control assessment to determine that Verkada performs control self-assessments at least annually to gain assurance that security controls are in place and operating effectively, and that corrective actions are taken based on relevant findings.	No exceptions noted.

CC4.2 - The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Number	Description of Control	Description of Test	Result of Testing
CC4.2.1	Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment and mitigation plans for remediation to determine that Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC4.2.2	Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	Inspected the annual penetration test and retest report to determine that Verkada engages with a third-party to conduct penetration tests of the production environment at least annually, that results are reviewed by management, and that there were no critical and high-priority findings to track through resolution.	No exceptions noted.
CC4.2.3	Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	<p>Inspected the quarterly vulnerability scan results to determine that Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly.</p> <p>Inspected the quarterly vulnerability scan results to determine that there were no critical or high-priority findings to track to resolution.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to tracking critical and high-priority findings to resolution, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>

Control Number	Description of Control	Description of Test	Result of Testing
CC4.2.4	Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Cybersecurity Incident Response Plan and the ticket for the security incident during the examination period to determine that Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	No exceptions noted.
CC4.2.5	Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC4.2.6	Verkada has implemented a Cybersecurity Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.	<p>Inspected the Cybersecurity Incident Response Plan to determine that Verkada has implemented an incident response policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.</p> <p>Inspected the list of security incidents identified during the examination period to determine that there were no PO incidents.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to performing a root cause analysis and reviewing lessons learned for PO security incidents, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>



Control Number	Description of Control	Description of Test	Result of Testing
CC4.2.7	The Security team communicates important information security events to company management in a timely manner.	Inspected the Security team's recurring meeting invites and the presentation deck from a meeting during the examination period to determine that the Security team communicates important information security events to company management in a timely manner.	No exceptions noted.

## CC5.0 - Common Criteria Related to Control Activities

CC5.1 - The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.1.1	Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Management Policy to determine that Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC5.1.2	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC5.1.3	Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment and mitigation plans for remediation to determine that Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.1.4	Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Security and Privacy Governance Committee Charter, the meeting agenda from a Committee meeting during the examination period, and Committee action items to determine that Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.
CC5.1.5	Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	No exceptions noted.

CC5.2 - The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.2.1	Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	No exceptions noted.
CC5.2.2	Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	Inspected the Security and Privacy Governance Committee Charter, the meeting agenda from a Committee meeting during the examination period, and Committee action items to determine that Verkada has an assigned Security team that is responsible for the design, implementation, management, and review of the organization's security policies, standards, baselines, procedures, and guidelines.	No exceptions noted.
CC5.2.3	Verkada restricts administrative access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio to authorized personnel based on job requirements.	Inspected the administrative user access lists for AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio and compared the users to the organizational chart to determine that Verkada restricts administrative access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio to authorized personnel based on job requirements.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.2.4	Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles which enables Verkada to restrict access to authorized personnel based on job titles.	Inspected the system integrations and role-based access configurations within Okta to determine that Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles which enables Verkada to restrict access to authorized personnel based on job titles.	No exceptions noted.
CC5.2.5	Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	Inspected the password, MFA, and SSO configurations to determine that Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.2.6	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	<p>Inspected Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the script for the rebuild of base images within the infrastructure as code repository twice a week in accordance with Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the GitHub Actions configurations that the security checks required to pass prior to new code being merged to master include a check that the build includes an approved image based on the approved image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p>	No exceptions noted.
CC5.2.7	Verkada configures security groups and load balancers to restrict access to production environment resources to authorized traffic.	Inspected the infrastructure configurations for security groups and load balancers to determine that Verkada configures security groups to restrict access to production environment resources to authorized traffic.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.2.8	Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days. Tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.	<p>Inspected the monitoring dashboard within one of Verkada's monitoring tools to determine that Verkada monitors host operating systems for vulnerabilities.</p> <p>Inspected the tickets logged within Verkada's ticketing system related to alerts for host operating system and container image vulnerabilities and for services running on container images that are older than 14 days to determine that Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days.</p> <p>Inspected the alerting and ticket creation configurations within Verkada's vulnerability monitoring tools to determine that tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.</p>	No exceptions noted.
CC5.2.9	Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	Inspected the annual penetration test and retest report to determine that Verkada engages with a third-party to conduct penetration tests of the production environment at least annually, that results are reviewed by management, and that there were no critical and high-priority findings to track through resolution.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.2.10	Verkada has an established policy and procedures that govern the use of cryptographic controls.	Inspected the Information Security Policy and Secrets Management Standard to determine that Verkada has an established policy and procedures that govern the use of cryptographic controls.	No exceptions noted.
CC5.2.11	Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Change Management Standard and Software Security Standard to determine that Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted.



CC5.3 - The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.3.1	Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	Inspected the Information Security Policy to determine that Verkada has a defined Information Security Policy that covers policies and procedures to support the functioning of internal control.	No exceptions noted.
CC5.3.2	Verkada Management has approved security policies, and all employees accept these procedures when hired.	<p>Inspected the security policy approval records to determine that Verkada Management has approved security policies.</p> <p>Inspected the accepted security policies for a selection of new hires to determine that employees accept these procedures when hired.</p>	No exceptions noted.
CC5.3.3	Verkada's Employee Handbook includes a formal Code of Conduct which is approved by management and accessible to all employees. Employees must sign the Employee Handbook upon hire.	Inspected the Employee Handbook and the signed Employee Handbook for a selection of new employees to determine that Verkada's Employee Handbook includes a formal Code of Conduct, which is approved by management and accessible to all employees, and that employees must sign the Employee Handbook upon hire.	No exceptions noted.
CC5.3.4	Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Management Policy to determine that Verkada has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.3.5	Verkada provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, along with any other complaints to the company management.	<p>Inspected the Cybersecurity Incident Response Plan and training content from the most recent annual security training to determine that Verkada provides a process to employees for reporting security, confidentiality, integrity, and availability features, incidents, and concerns, along with any other complaints to the company management.</p> <p>Reperformed the submission of an email sent to Security@verkada.com to determine that Verkada maintains a Security@ email alias for employees to submit concerns, events, and issues to Verkada management for resolution.</p>	No exceptions noted.
CC5.3.6	Verkada has an established Cybersecurity Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has an established Cybersecurity Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC5.3.7	Verkada has a Data Deletion Policy to help guide the deletion of customer data.	Inspected the Data Deletion Policy to determine that Verkada has a Data Deletion Policy to help guide the deletion of customer data.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC5.3.8	Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Change Management Standard and Software Security Standard to determine that Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted.
CC5.3.9	Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	Inspected the Vendor Risk and Compliance Management Policy to determine that Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	No exceptions noted.
CC5.3.10	Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.

## CC6.0 - Common Criteria Related to Logical and Physical Access Controls

CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.1.1	Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles which enables Verkada to restrict access to authorized personnel based on job titles.	Inspected the system integrations and role-based access configurations within Okta to determine that Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles which enables Verkada to restrict access to authorized personnel based on job titles.	No exceptions noted.
CC6.1.2	Data stored in S3 buckets, RDS databases, and Backblaze databases is encrypted at rest.	Inspected the encryption configurations for S3, RDS, and Backblaze to determine that data stored in S3 buckets, RDS databases, and Backblaze databases is encrypted at rest.	No exceptions noted.
CC6.1.3	Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	Inspected the password, MFA, and SSO configurations to determine that Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	No exceptions noted.
CC6.1.4	Verkada's Command Platform user passwords are stored using a salted password hash.	Inspected the password source code to determine that Verkada's Command Platform user passwords are stored using a salted password hash.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.1.5	Verkada ensures that company-issued laptops have encrypted hard-disks.	<p>Inspected the MDM security policies configured within the MDM tools to determine that Verkada ensures that company-issued laptops have encrypted hard-disks.</p> <p>Inspected the security policies enforced on a selection of laptops to determine that Verkada ensures that company-issued laptops have encrypted hard-disks.</p>	No exceptions noted.
CC6.1.6	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	<p>Inspected Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the script for the rebuild of base images within the infrastructure as code repository twice a week in accordance with Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the GitHub Actions configurations that the security checks required to pass prior to new code being merged to master include a check that the build includes an approved image based on the approved image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p>	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.1.7	Verkada configures security groups and load balancers to restrict access to production environment resources to authorized traffic.	Inspected the infrastructure configurations for security groups and load balancers to determine that Verkada configures security groups to restrict access to production environment resources to authorized traffic.	No exceptions noted.
CC6.1.8	Verkada configures NACLs at the subnet level to help restrict access to authorized traffic.	Inspected the NACL configurations for the production VPCs to determine that Verkada configures NACLs at the subnet level to help restrict access to authorized traffic.	No exceptions noted.
CC6.1.9	MDM systems are in place to centrally manage mobile devices supporting the service.	Inspected the MDM systems' security policies to determine that MDM systems are in place to centrally manage mobile devices supporting the service.	No exceptions noted.

CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.2.1	Verkada uses role-based access through Okta to provision access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	Inspected Okta and role-based permissions configured configuration files to determine that Verkada uses role-based access through Okta to provision access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	No exceptions noted.
CC6.2.2	Verkada performs user access control reviews for AWS, Backblaze, GitHub, Argo CD, and the Command Platform annually, at minimum.	Inspected the completed annual user access control review ticket to determine that Verkada performs user access control reviews for AWS, Backblaze, GitHub, Argo CD, and the Command Platform annually, at minimum.	No exceptions noted.
CC6.2.3	System access is removed from terminated employees within one business day. Employee devices are locked as part of the offboarding process.	Inspected the offboarding ticket and access removal configuration for a selection of terminated employees to determine that system access is removed from terminated employees within one business day and that employee devices are locked as part of the offboarding process.	No exceptions noted.

CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.3.1	Verkada uses role-based access through Okta to provision access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	Inspected Okta and role-based permissions configured configuration files to determine that Verkada uses role-based access through Okta to provision access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	No exceptions noted.
CC6.3.2	Verkada restricts administrative access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio to authorized personnel based on job requirements.	Inspected the administrative user access lists for AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio and compared the users to the organizational chart to determine that Verkada restricts administrative access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio to authorized personnel based on job requirements.	No exceptions noted.
CC6.3.3	Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles which enables Verkada to restrict access to authorized personnel based on job titles.	Inspected the system integrations and role-based access configurations within Okta to determine that Verkada uses role-based access to manage user access to AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio which enables Verkada to restrict access to authorized personnel based on job titles which enables Verkada to restrict access to authorized personnel based on job titles.	No exceptions noted.



Control Number	Description of Control	Description of Test	Result of Testing
CC6.3.4	Verkada performs user access control reviews for AWS, Backblaze, GitHub, Argo CD, and the Command Platform annually, at minimum.	Inspected the completed annual user access control review ticket to determine that Verkada performs user access control reviews for AWS, Backblaze, GitHub, Argo CD, and the Command Platform annually, at minimum.	No exceptions noted.
CC6.3.5	System access is removed from terminated employees within one business day. Employee devices are locked as part of the offboarding process.	Inspected the offboarding ticket and access removal configuration for a selection of terminated employees to determine that system access is removed from terminated employees within one business day and that employee devices are locked as part of the offboarding process.	No exceptions noted.

CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.4.1	Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	Inspected the Vendor Risk and Compliance Management Policy to determine that Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	No exceptions noted.
CC6.4.2	Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected Verkada's vendor directory and the terms of service for a selection of high-risk vendors to determine that Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted.

CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.5.1	Verkada has a Data Deletion Policy to help guide the deletion of customer data.	Inspected the Data Deletion Policy to determine that Verkada has a Data Deletion Policy to help guide the deletion of customer data.	No exceptions noted.
CC6.5.2	System access is removed from terminated employees within one business day. Employee devices are locked as part of the offboarding process.	Inspected the offboarding ticket and access removal configuration for a selection of terminated employees to determine that system access is removed from terminated employees within one business day and that employee devices are locked as part of the offboarding process.	No exceptions noted.

CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.6.1	Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	Inspected the password, MFA, and SSO configurations to determine that Verkada enforces minimum password length, password complexity, and multi-factor authentication (MFA) for user login AWS, Backblaze, GitHub, Argo CD, the Command Platform, Cloudflare, and Twilio.	No exceptions noted.
CC6.6.2	MDM systems are in place to centrally manage mobile devices supporting the service.	Inspected the MDM systems' security policies to determine that MDM systems are in place to centrally manage mobile devices supporting the service.	No exceptions noted.
CC6.6.3	Verkada configures security groups and load balancers to restrict access to production environment resources to authorized traffic.	Inspected the infrastructure configurations for security groups and load balancers to determine that Verkada configures security groups to restrict access to production environment resources to authorized traffic.	No exceptions noted.
CC6.6.4	Verkada configures NACLs at the subnet level to help restrict access to authorized traffic.	Inspected the NACL configurations for the production VPCs to determine that Verkada configures NACLs at the subnet level to help restrict access to authorized traffic.	No exceptions noted.
CC6.6.5	An IDS is in place to detect potential intrusions and alert personnel when a potential intrusion is detected.	Inspected the IDS tool dashboard, alerting configurations, and an example alert to determine that an IDS is in place to detect potential intrusions and alert personnel when a potential intrusion is detected.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.6.6	Verkada ensures that all company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	Inspected the screensaver lockout configurations within the MDM tools and the security policies enforced on a selection of laptops to determine that Verkada ensures that company-issued computers use a screensaver lock with a timeout of no more than 15 minutes.	No exceptions noted.
CC6.6.7	Read/write access to S3 buckets and Backblaze is configured to restrict public access.	Inspected the Verkada's S3 bucket and Backblaze configurations to determine that read/write access to S3 buckets and Backblaze is configured to restrict public access.	No exceptions noted.

CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.7.1	Verkada ensures that all connections to its web application from its users are encrypted.	Inspected the infrastructure configurations and the web application encryption certificate to determine that Verkada ensures that all connections to its web application from its users are encrypted.	No exceptions noted.
CC6.7.2	Verkada enforces secure transmission of information when sending data to the cloud storage provider.	Inspected the code that enforces the encrypted connection to the cloud storage provider to determine that Verkada enforces secure transmission of information when sending data to the cloud storage provider.	No exceptions noted.
CC6.7.3	Verkada enforces secure and encrypted connections when accessing production and staging resources.	Inspected the Cloudflare infrastructure configurations to determine that Verkada enforces secure and encrypted connections when accessing production and staging resources.	No exceptions noted.
CC6.7.4	Data stored in S3 buckets, RDS databases, and Backblaze databases is encrypted at rest.	Inspected the encryption configurations for S3, RDS, and Backblaze to determine that data stored in S3 buckets, RDS databases, and Backblaze databases is encrypted at rest.	No exceptions noted.
CC6.7.5	Verkada's customer data is segregated from the data of other customers.	Inspected snippets of Verkada code demonstrating the logical segregation of customer data within the application and AWS S3 objects to determine that Verkada's customer data is segregated from the data of other customers.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.7.6	MDM systems are in place to centrally manage mobile devices supporting the service.	Inspected the MDM systems' security policies to determine that MDM systems are in place to centrally manage mobile devices supporting the service.	No exceptions noted.
CC6.7.7	Verkada ensures that company-issued laptops have encrypted hard-disks.	<p>Inspected the MDM security policies configured within the MDM tools to determine that Verkada ensures that company-issued laptops have encrypted hard-disks.</p> <p>Inspected the security policies enforced on a selection of laptops to determine that Verkada ensures that company-issued laptops have encrypted hard-disks.</p>	No exceptions noted.

CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.8.1	Verkada requires antivirus software to be installed on workstations to protect the network against malware.	Inspected evidence of antivirus installed on a selection of workstations to determine that Verkada requires antivirus software to be installed on workstations to protect the network against malware.	No exceptions noted.
CC6.8.2	Verkada's workstation operating system security patches are applied automatically.	<p>Inspected the MDM security policies configured within the MDM tools to determine that Verkada's workstation operating system security patches are applied automatically.</p> <p>Inspected the OS version and evidence of the auto-update configuration enforced for a selection of workstations to determine that Verkada's workstation operating system security patches are applied automatically.</p>	No exceptions noted.



Control Number	Description of Control	Description of Test	Result of Testing
CC6.8.3	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	<p>Inspected Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the script for the rebuild of base images within the infrastructure as code repository twice a week in accordance with Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the GitHub Actions configurations that the security checks required to pass prior to new code being merged to master include a check that the build includes an approved image based on the approved image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p>	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.8.4	Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days. Tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.	<p>Inspected the monitoring dashboard within one of Verkada's monitoring tools to determine that Verkada monitors host operating systems for vulnerabilities.</p> <p>Inspected the tickets logged within Verkada's ticketing system related to alerts for host operating system and container image vulnerabilities and for services running on container images that are older than 14 days to determine that Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days.</p> <p>Inspected the alerting and ticket creation configurations within Verkada's vulnerability monitoring tools to determine that tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.</p>	No exceptions noted.
CC6.8.5	Verkada ensures that file integrity monitoring (FIM) software is in place to detect whether operating system and application software files have been tampered with.	Inspected the FIM software configuration to determine that Verkada ensures FIM software is in place to detect whether operating system and application software files have been tampered with.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC6.8.6	Verkada has configured a SIEM tools that collects and stores server logs in a central location. Access to the logs stored in the SIEM tools is restricted to authorized users.	Inspected the SIEM tools configurations and the list of users with access to the SIEM tools and compared to the list of employees to determine that Verkada has configured SIEM tools that collect and store server logs in a central location, and that access to the logs stored in the SIEM tools is restricted to authorized users.	No exceptions noted.
CC6.8.7	Verkada has configured its SIEM tools to send alerts to the business communications channel to alert the appropriate teams when anomalous system events occur. The SIEM tools are also configured to automatically create a ticket in their issue and project tracking software when critical and high-severity events occur, where the events are logged and tracked through resolution.	<p>Inspected the SIEM tools alerting configurations to determine that Verkada has configured its SIEM tools to send alerts to the business communications channel when anomalous system events occur and that a ticket is automatically created in their project tracking software when critical or high-severity events occur.</p> <p>Inspected the list of critical and high-severity issue tickets to determine that critical and high-severity security events are logged and tracked through resolution.</p>	No exceptions noted.

## CC7.0 - Common Criteria Related to System Operations

CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.1.1	Verkada has enabled infrastructure logs throughout their production environment. Infrastructure logs are stored encrypted, log file validation is enabled, and access to infrastructure logs is restricted to those who require access to perform their job duties.	Inspected the infrastructure configurations and the list of users with access to the infrastructure logs and compared users to the list of employees to determine that Verkada has enabled infrastructure logs throughout their production environment, infrastructure logs are stored encrypted, log file validation is enabled, and access to infrastructure logs is restricted to those who require access to perform their job duties.	No exceptions noted.
CC7.1.2	Verkada has configured a SIEM tools that collects and stores server logs in a central location. Access to the logs stored in the SIEM tools is restricted to authorized users.	Inspected the SIEM tools configurations and the list of users with access to the SIEM tools and compared to the list of employees to determine that Verkada has configured SIEM tools that collect and store server logs in a central location, and that access to the logs stored in the SIEM tools is restricted to authorized users.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.1.3	Verkada has configured its SIEM tools to send alerts to the business communications channel to alert the appropriate teams when anomalous system events occur. The SIEM tools are also configured to automatically create a ticket in their issue and project tracking software when critical and high-severity events occur, where the events are logged and tracked through resolution.	<p>Inspected the SIEM tools alerting configurations to determine that Verkada has configured its SIEM tools to send alerts to the business communications channel when anomalous system events occur and that a ticket is automatically created in their project tracking software when critical or high-severity events occur.</p> <p>Inspected the list of critical and high-severity issue tickets to determine that critical and high-severity security events are logged and tracked through resolution.</p>	No exceptions noted.
CC7.1.4	Verkada engages with a third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	Inspected the annual penetration test and retest report to determine that Verkada engages with a third-party to conduct penetration tests of the production environment at least annually, that results are reviewed by management, and that there were no critical and high-priority findings to track through resolution.	No exceptions noted.
CC7.1.5	Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly. Results are reviewed by management and critical and high-priority findings are tracked to resolution.	<p>Inspected the quarterly vulnerability scan results to determine that Verkada engages with a third-party to conduct vulnerability scans of the production environment at least quarterly.</p> <p>Inspected the quarterly vulnerability scan results to determine that there were no critical or high-priority findings to track to resolution.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to tracking critical and high-priority findings to resolution, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>

Control Number	Description of Control	Description of Test	Result of Testing
CC7.1.6	Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days. Tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.	<p>Inspected the monitoring dashboard within one of Verkada's monitoring tools to determine that Verkada monitors host operating systems for vulnerabilities.</p> <p>Inspected the tickets logged within Verkada's ticketing system related to alerts for host operating system and container image vulnerabilities and for services running on container images that are older than 14 days to determine that Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days.</p> <p>Inspected the alerting and ticket creation configurations within Verkada's vulnerability monitoring tools to determine that tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.</p>	No exceptions noted.

CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.2.1	Verkada has enabled infrastructure logs throughout their production environment. Infrastructure logs are stored encrypted, log file validation is enabled, and access to infrastructure logs is restricted to those who require access to perform their job duties.	Inspected the infrastructure configurations and the list of users with access to the infrastructure logs and compared users to the list of employees to determine that Verkada has enabled infrastructure logs throughout their production environment, infrastructure logs are stored encrypted, log file validation is enabled, and access to infrastructure logs is restricted to those who require access to perform their job duties.	No exceptions noted.
CC7.2.2	Verkada has configured a SIEM tools that collects and stores server logs in a central location. Access to the logs stored in the SIEM tools is restricted to authorized users.	Inspected the SIEM tools configurations and the list of users with access to the SIEM tools and compared to the list of employees to determine that Verkada has configured SIEM tools that collect and store server logs in a central location, and that access to the logs stored in the SIEM tools is restricted to authorized users.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.2.3	Verkada has configured its SIEM tools to send alerts to the business communications channel to alert the appropriate teams when anomalous system events occur. The SIEM tools are also configured to automatically create a ticket in their issue and project tracking software when critical and high-severity events occur, where the events are logged and tracked through resolution.	<p>Inspected the SIEM tools alerting configurations to determine that Verkada has configured its SIEM tools to send alerts to the business communications channel when anomalous system events occur and that a ticket is automatically created in their project tracking software when critical or high-severity events occur.</p> <p>Inspected the list of critical and high-severity issue tickets to determine that critical and high-severity security events are logged and tracked through resolution.</p>	No exceptions noted.
CC7.2.4	Verkada has configured a cloud observability service to monitor their cloud infrastructure for system performance issues. Critical and high-severity alerts are sent to the incident response tool to alert the on-call engineer.	Inspected the cloud observability service alert configurations, the on-call schedule, an example performance alert, and evidence that the alert was logged and tracked through a resolution to determine that Verkada has configured a cloud observability service to monitor their cloud infrastructure for system performance issues and that critical and high severity alerts are sent to the incident response tool to alert the on-call engineer.	No exceptions noted.



CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.3.1	Verkada has configured its SIEM tools to send alerts to the business communications channel to alert the appropriate teams when anomalous system events occur. The SIEM tools are also configured to automatically create a ticket in their issue and project tracking software when critical and high-severity events occur, where the events are logged and tracked through resolution.	<p>Inspected the SIEM tools alerting configurations to determine that Verkada has configured its SIEM tools to send alerts to the business communications channel when anomalous system events occur and that a ticket is automatically created in their project tracking software when critical or high-severity events occur.</p> <p>Inspected the list of critical and high-severity issue tickets to determine that critical and high-severity security events are logged and tracked through resolution.</p>	No exceptions noted.
CC7.3.2	Verkada has configured a cloud observability service to monitor their cloud infrastructure for system performance issues. Critical and high-severity alerts are sent to the incident response tool to alert the on-call engineer.	Inspected the cloud observability service alert configurations, the on-call schedule, an example performance alert, and evidence that the alert was logged and tracked through a resolution to determine that Verkada has configured a cloud observability service to monitor their cloud infrastructure for system performance issues and that critical and high severity alerts are sent to the incident response tool to alert the on-call engineer.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.3.3	Security incidents are logged, tracked, resolved, and communicated to affected parties by management according to Verkada's security incident response policies and procedures. All security incidents are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.	<p>Inspected the Cybersecurity Incident Response Plan to determine that security incidents are logged, tracked, resolved, and communicated to affected parties by management according to the company's security incident response policies and procedures and that all incidents are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.</p> <p>Inspected Linear tickets for a selection of security incidents that occurred during the examination period to determine that security incidents are logged, tracked, resolved, and communicated to affected parties by management according to the company's security incident response policies and procedures and that all incidents are evaluated to determine whether they could have resulted in a failure to meet security commitments and objectives.</p>	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.3.4	Verkada has implemented a Cybersecurity Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.	<p>Inspected the Cybersecurity Incident Response Plan to determine that Verkada has implemented an incident response policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.</p> <p>Inspected the list of security incidents identified during the examination period to determine that there were no PO incidents.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to performing a root cause analysis and reviewing lessons learned for PO security incidents, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>
CC7.3.5	Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC7.3.6	Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Cybersecurity Incident Response Plan and the ticket for the security incident during the examination period to determine that Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.3.7	Verkada has an established Cybersecurity Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has an established Cybersecurity Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.

CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.4.1	Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Cybersecurity Incident Response Plan and the ticket for the security incident during the examination period to determine that Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	No exceptions noted.
CC7.4.2	Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC7.4.3	Verkada has an established Cybersecurity Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has an established Cybersecurity Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.4.4	Verkada has implemented a Cybersecurity Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.	<p>Inspected the Cybersecurity Incident Response Plan to determine that Verkada has implemented an incident response policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.</p> <p>Inspected the list of security incidents identified during the examination period to determine that there were no PO incidents.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to performing a root cause analysis and reviewing lessons learned for PO security incidents, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>

CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.5.1	Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	Inspected the Cybersecurity Incident Response Plan and the ticket for the security incident during the examination period to determine that Verkada has implemented a Cybersecurity Incident Response Plan that includes steps for creating, prioritizing, assigning, and tracking follow-ups to completion.	No exceptions noted.
CC7.5.2	Verkada has an established Cybersecurity Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has an established Cybersecurity Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC7.5.3	Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has identified an incident response team that quantifies and monitors incidents involving security, availability, processing integrity, and confidentiality at the company.	No exceptions noted.
CC7.5.4	Verkada ensures that incident response plan testing is performed on an annual basis.	Inspected the Verkada Incident Response Tabletop Exercise slides and the calendar meeting invitation supporting Verkada's most recent incident response tabletop exercise to determine that Verkada performs incident response plan testing annually.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC7.5.5	Verkada has implemented a Cybersecurity Incident Response Plan that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.	<p>Inspected the Cybersecurity Incident Response Plan to determine that Verkada has implemented an incident response policy that includes documenting "Lessons Learned" and "Root Cause Analysis" after PO security incidents and sharing them with the broader engineering team.</p> <p>Inspected the list of security incidents identified during the examination period to determine that there were no PO incidents.</p>	<p>No exceptions noted.</p> <p>The circumstances that warrant the operation of this control, as it relates to performing a root cause analysis and reviewing lessons learned for PO security incidents, did not occur during the examination period and, as a result, the operating effectiveness of this control could not be tested.</p>
CC7.5.6	Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.
CC7.5.7	Verkada performs database backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Information Security Policy and database backup configurations to determine that Verkada performs database backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	No exceptions noted.
CC7.5.8	Verkada conducts annual disaster recovery tests and documents results according to the Disaster Recovery Plan.	Inspected the Disaster Recovery Plan and tabletop test results from the most recent annual disaster recovery test to determine that Verkada conducts annual disaster recovery tests and documents results according to the Disaster Recovery Plan.	No exceptions noted.



## CC8.0 - Common Criteria Related to Change Management

CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Number	Description of Control	Description of Test	Result of Testing
CC8.1.1	Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Change Management Standard and Software Security Standard to determine that Verkada has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted.
CC8.1.2	Separate environments are used for testing and production for Verkada's application.	Inspected Verkada's logically separated AWS accounts to determine that separate environments are used for testing and production for Verkada's application.	No exceptions noted.
CC8.1.3	Verkada uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	Inspected the version control system to determine that Verkada uses a version control system to manage source code, documentation, release labeling, and other change management tasks.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC8.1.4	Verkada systematically requires code changes to undergo code reviews and tests prior to merging to the master branch by someone other than the person who made the code change.	Inspected the branch protection rules for each in-scope repository, the GitHub Action configurations for each in-scope repository, and example merged commits from each in-scope repository to determine that Verkada systematically requires code changes to undergo code reviews and tests prior to merging to the master branch by someone other than the person who made the code change.	No exceptions noted.
CC8.1.5	Verkada ensures that code changes are tested prior to implementation to ensure quality and security.	<p>Inspected the branch protection rules for each in-scope repository, the GitHub Action configurations for each in-scope repository, and example merged commits from each in-scope repository to determine that Verkada ensures that code changes are tested prior to implementation to ensure quality and security.</p> <p>Inspected the code supporting Verkada's software composition analysis tool and evidence that the tool is configured to automatically resolve identified code vulnerabilities in accordance with established conditions for merging to determine that Verkada ensures that code changes are tested prior to implementation to ensure quality and security.</p>	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC8.1.6	Verkada ensures that releases are approved by code owners prior to merging into the master branch.	Inspected the branch protection rules for each in-scope repository and example merged commits from each in-scope repository to determine that Verkada systematically requires code changes to be reviewed and approved by a code owner prior to merging to the master branch.	No exceptions noted.
CC8.1.7	Verkada restricts deployment permissions to engineers through role-based access	Inspected the deployment tool role-based access permissions to determine that Verkada restricts deployment permissions to engineers through role-based access.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC8.1.8	Hardening standards are in place to ensure that newly deployed server instances are appropriately secured.	<p>Inspected Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the script for the rebuild of base images within the infrastructure as code repository twice a week in accordance with Verkada's approved base image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p> <p>Inspected the GitHub Actions configurations that the security checks required to pass prior to new code being merged to master include a check that the build includes an approved image based on the approved image file to determine that hardening standards are in place to ensure that newly deployed server instances are appropriately secured.</p>	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC8.1.9	Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days. Tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.	<p>Inspected the monitoring dashboard within one of Verkada's monitoring tools to determine that Verkada monitors host operating systems for vulnerabilities.</p> <p>Inspected the tickets logged within Verkada's ticketing system related to alerts for host operating system and container image vulnerabilities and for services running on container images that are older than 14 days to determine that Verkada monitors host operating systems and container images for vulnerabilities and for services running on container images that are older than 14 days.</p> <p>Inspected the alerting and ticket creation configurations within Verkada's vulnerability monitoring tools to determine that tickets are automatically created for identified vulnerabilities and for services requiring redeployment because the container images are older than 14 days.</p>	No exceptions noted.

## CC9.0 - Common Criteria Related to Risk Mitigation

CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control Number	Description of Control	Description of Test	Result of Testing
CC9.1.1	Verkada conducts a formal risk assessment which is reviewed at least annually.	Inspected the annual risk assessment and the Security and Privacy Committee meeting minutes to determine that Verkada conducts a formal risk assessment which is reviewed at least annually.	No exceptions noted.
CC9.1.2	Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the risk assessment and mitigation plans for remediation to determine that Verkada's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC9.1.3	Verkada performs database backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	Inspected the Information Security Policy and database backup configurations to determine that Verkada performs database backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	No exceptions noted.
CC9.1.4	Verkada conducts annual disaster recovery tests and documents results according to the Disaster Recovery Plan.	Inspected the Disaster Recovery Plan and tabletop test results from the most recent annual disaster recovery test to determine that Verkada conducts annual disaster recovery tests and documents results according to the Disaster Recovery Plan.	No exceptions noted.

Control Number	Description of Control	Description of Test	Result of Testing
CC9.1.5	Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that Verkada has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.
CC9.1.6	Verkada has an established Cybersecurity Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the Cybersecurity Incident Response Plan to determine that Verkada has an established Cybersecurity Incident Response Policy that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC9.1.7	Verkada ensures that incident response plan testing is performed on an annual basis.	Inspected the Verkada Incident Response Tabletop Exercise slides and the calendar meeting invitation supporting Verkada's most recent incident response tabletop exercise to determine that Verkada performs incident response plan testing annually.	No exceptions noted.
CC9.1.8	Verkada maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the cybersecurity insurance policy to determine that Verkada maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.

## CC9.2 - The entity assesses and manages risks associated with vendors and business partners.

Control Number	Description of Control	Description of Test	Result of Testing
CC9.2.1	Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	Inspected the Vendor Risk and Compliance Management Policy to determine that Verkada has a Vendor Risk and Compliance Management Policy to help define and assess vendor risk, implement controls to mitigate vendor-related risks, and manage vendor relationships.	No exceptions noted.
CC9.2.2	Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	Inspected Verkada's vendor directory and the terms of service for a selection of high-risk vendors to determine that Verkada maintains a directory of its key vendors, including its agreements that specify terms, conditions and responsibilities.	No exceptions noted.
CC9.2.3	Verkada maintains a directory of its key vendors, including their compliance reports. High-risk vendor compliance reports are reviewed annually.	Inspected Verkada's vendor directory and the due diligence performed for a selection of high-risk vendors to determine that Verkada maintains a directory of its key vendors, including their compliance reports, and that high-risk vendor compliance reports are reviewed annually.	<p>Exceptions noted.</p> <p>For three out of seven high-risk vendors selected for testing, the review of compliance reports was not documented.</p> <p>For four out of seven high-risk vendors selected for testing, the review of compliance reports was not complete and accurate.</p>



## V. Other Information Provided by Verkada That is Not Covered by the Service Auditor's Report

## Management's Responses to Control Exceptions

Control Number	Controls Specified by Verkada, Inc.	Results of Tests	Management Response
CC3.2.4, CC4.1.3, CC6.4.3, CC9.2.3	Verkada maintains a directory of its key vendors, including their compliance reports. High-risk vendor compliance reports are reviewed annually.	<p>For three out of seven high-risk vendors selected for testing, the review of compliance reports was not documented.</p> <p>For four out of seven high-risk vendors selected for testing, the review of compliance reports was not complete and accurate.</p>	To address these findings, we have updated the standardized vendor security review procedure to include specific documentation of report details, impact assessments, control validation, and vendor review record keeping. All high-risk vendors identified in the audit have since been reviewed according to this updated procedure.



# How Verkada Supports HIPAA Compliance



## Background

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect the use and disclosure of medical records and other individually identifiable health information. It established national standards for the protection of sensitive health records. These protections were later extended to electronic health records in 2009 through the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

### Who must comply with HIPAA?

The Department of Health and Human Services stipulates that HIPAA must be followed by all “covered entities” including:

- Healthcare Providers (including hospitals, medical centers, clinics, physicians, pharmacies and nursing homes)
- Health Plans (including company health insurers, health plans, health maintenance organizations (HMOs) and government programs that pay for healthcare)
- Healthcare Clearinghouses

and their vendors who process PHI on their behalf, also known as “business associates.”

### How is HIPAA enforced?

HIPAA is enforced primarily by The Department of Health and Human Services-Office for Civil Rights (OCR). The HITECH Act extends similar investigative authority to the State Attorneys General. Upon receiving a complaint or report of a security breach, the OCR begins conducting an investigation or general audit depending on the severity and specificity of the violation. Serious cases of non-compliance can result in substantial fines and penalties (in excess of 1.5 million per year) and potential criminal charges.



## Title II – The Administrative Simplification Provisions

Title II of HIPAA codifies rules for maintaining the security and privacy of individually identifiable health information. These provisions, known as the Administrative Simplification rules, require the Department of Health and Human Services (HHS) to establish specific standards for the protection and use of healthcare information. Accordingly, the HHS created a number of rules that have become the basis for what most refer to as HIPAA compliance.

### The Privacy Rule

Since the adoption of HIPAA, the HHS has established a number of regulations for the access and disclosure of medical records and other individually identifiable health information, referred to as protected health information (PHI). These regulations are collectively known as “the Privacy Rule.”

In limited circumstances, video surveillance footage can be considered PHI if it can be used to *directly identify* an individual and their treatment. This could include footage from a patient’s room or from another treatment area such as an operating room. However, footage of common areas such as entrance ways, waiting rooms, or storage closets is not considered PHI and can be shared or stored with fewer restrictions.

For more guidance see [www.hhs.gov/hipaa/for-professionals/security/guidance/index.html](https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html)

### The Security Rule

In order to protect and ensure the privacy afforded to patients by the Privacy Rule, HHS published Security Standards for the Protection of Electronic Protected Health Information (e-PHI), also referred to as “the Security Rule.” As the title implies, the Security Rule extends protections of the Privacy Rule to records that are stored and transferred electronically rather than physically.

Specifically, covered entities and their business associates must:

- Ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance by their workforce





## HIPAA Administrative Safeguards

### Security management process

#### [45 C.F.R. § 164.306(e)]

A covered entity must identify and analyze potential risks to e-PHI and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

## How Verkada Helps

Verkada Surveillance and Access Control systems can be used to actively monitor secure sites where e-PHI is accessed or stored.

Verkada performs regular security audits of its storage and transfer of data, including e-PHI. Read more about Verkada Security at [www.verkada.com/security](https://www.verkada.com/security)

### Information Access Management

#### [45 C.F.R. § 164.308(a)(4)(i)]

Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the “minimum necessary,” the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient’s role (role-based access)

Verkada Command features Role Based Access Control (RBAC), allowing for least privileged access permissions granted on the individual and organizational level.

### Information Access Management

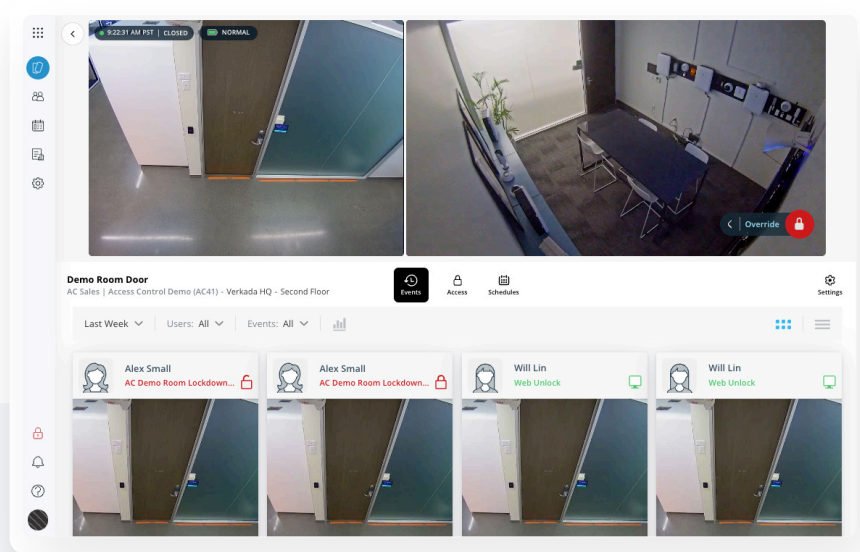
#### [45 C.F.R. § 164.308(a)(4)(i)]

A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Verkada systems are simple to set up and operate, making user training easy to perform.



## Physical Safeguards



### Facility Access and Control

#### [45 C.F.R. § 164.310(a)]

A covered entity must identify and analyze potential risks to e-PHI and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

### How Verkada Helps

Verkada Cameras and Access Control can be installed in key locations, such as workstations, to actively monitor how they're being used.

### Workstation and Device Security

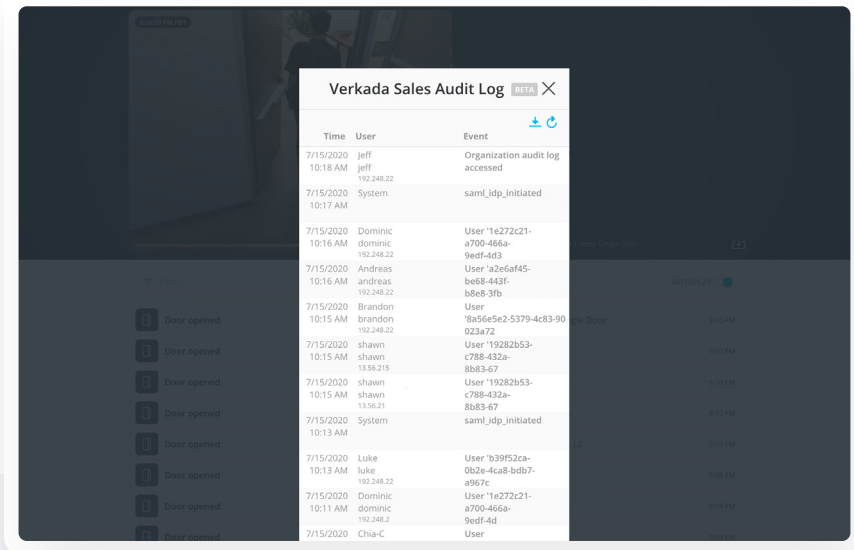
#### [45 C.F.R. § 164.308(a)(2)]

A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

Verkada Access Control makes it easy to assign physical access to only the right parties. Tiered, role-based permissions simplify the process of giving new users the correct level of access.



## Technical Safeguards



Verkada Sales Audit Log <span>BETA</span> <span>×</span>		
Time	User	Event
7/15/2020 10:18 AM	jeff jeff 192.248.22	Organization audit log accessed
7/15/2020 10:17 AM	System	saml_idp_initiated
7/15/2020 10:16 AM	Dominic dominic 192.248.22	User '1e272c21-a700-466a-9edf-4d3
7/15/2020 10:16 AM	Andreas andreas 192.248.22	User 'a2e6af45-be68-443f-b8e8-3fb
7/15/2020 10:15 AM	Brandon brandon 192.248.22	User '8a56e5e2-5379-4c83-90023a72
7/15/2020 10:15 AM	shawn shawn 13.56.215	User '19282b53-c788-432a-8b83-67
7/15/2020 10:15 AM	shawn shawn 13.56.21	User '19282b53-c788-432a-8b83-67
7/15/2020 10:13 AM	System	saml_idp_initiated
7/15/2020 10:13 AM	Luke luke 192.248.22	User 'b39f52ca-0b2e-4ca8-bdb7-a967c
7/15/2020 10:11 AM	Dominic dominic 192.248.2	User '1e272c21-a700-466a-9edf-4d
7/15/2020	Chia-C	User

### Access Control

#### [45 C.F.R. § 164.312(a)]

A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

## How Verkada Helps

Verkada Access Control includes a tiered role-based model to help ensure only authorized persons access e-PHI. Verkada also integrates with the most trusted Single Sign-On identity providers in the industry. Traditional Multi-Factor Authentication is available to enhance access controls.

### Audit Controls

#### [45 C.F.R. § 164.308(a)(2)]

A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Verkada Command features comprehensive audit logs that record the identity of anyone who has accessed the system and any changes that they have made.

### Integrity Controls

#### [45 C.F.R. § 164.312(c)]

A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to con rm that e-PHI has not been improperly altered or destroyed.

Verkada data is stored redundantly across multiple local AWS servers. In the unlikely event that one data center is compromised or disabled, e-PHI will be preserved in other in-region data centers.





**Transmission Security**  
**[45 C.F.R. § 164.312(E)]**

A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network

**How Verkada Helps**

All Verkada data is encrypted in transit using the AES 128 and TLS v1.2 algorithms, whether footage is being sent to the cloud or accessed by a mobile device.

**Verkada is Trusted by Over  
250 Healthcare Organizations**













Want to learn more about Verkada's physical security solution?

Get a Free Trial

# Verkada ISMS Statement of Applicability 1.0

The Statement of Applicability (SOA) links Verkada's risk assessment and treatment with the implementation of the ISMS. It provides the company with an overview of what needs to be done in information security, why, and how.

The SOA will list all Annex A controls that are applicable and those that are not. Each control decision will have a justification as to whether they were implemented, why and where (see below).

## ISO 27001

CONTROL	OBJECTIVE & DESCRIPTION	STATUS (Applicable /Not Applicable)	Legal Requirement (Y/N)	Contractual Obligation (Y/N)	Business Requirement/ Best Practice (Y/N)	Results of Risk Assessment (Y/N)	IMPLEMENTATION (Y/N)	REMARKS	RESPONSIBLE ENTITY (Dept/Role)
A.5	INFORMATION SECURITY POLICIES								
A.5.1	Policies for information security Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned	Applicable	N	N	Y	Y	Y		Verkada Security & Privacy Governance Committee

	intervals and if significant changes occur.							
A.5.2	Information security roles and responsibilities Information security roles and responsibilities should be defined and allocated according to the organization needs.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.3	Segregation of duties Conflicting duties and conflicting areas of responsibility should be segregated.	Applicable	N	N	Y	Y	Y	Verkada Security Team, Verkada Engineering Team
A.5.4	Management responsibilities Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	Applicable	N	N	Y	Y	Y	Verkada Security & Privacy Governance Committee
A.5.5	Contact with authorities The organization should establish and maintain contact with relevant authorities.	Applicable	N	N	Y	Y	Y	Verkada Security & Privacy Governance Committee

A.5.6	Contact with special interest groups The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Applicable	N	N	Y	Y	Y	Verkada Security & Privacy Governance Committee
A.5.7	Threat intelligence Information relating to information security threats should be collected and analysed to produce threat intelligence.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.8	Information security in project management Information security should be integrated into project management.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.9	Inventory of information and other associated assets An inventory of information and other associated assets, including owners, should be developed and maintained.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.10	Acceptable use of information and other associated assets Rules for the acceptable use and procedures for handling information and other associated	Applicable	N	N	Y	Y	Y	Verkada Security & Privacy Governance Committee

	assets should be identified, documented and implemented.							
A.5.11	Return of assets Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	Applicable	N	N	Y	Y	Y	Verkada IT Team
A.5.12	Classification of information Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.13	Labeling of information An appropriate set of procedures for information labeling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable	N	N	Y	Y	Y	Verkada Privacy Verkada Security
A.5.14	Information transfer Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization	Applicable	N	N	Y	Y	Y	Verkada Legal Team

	and between the organization and other parties.							
A.5.15	<p>Access control</p> <p>Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.</p>	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.16	<p>Identity management</p> <p>The full life cycle of identities should be managed.</p>	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team
A.5.17	<p>Authentication information</p> <p>Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.</p>	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team
A.5.18	<p>Access rights</p> <p>Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific</p>	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team

	policy on and rules for access control.							
A.5.19	Information security in supplier relationships Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Applicable	N	N	Y	Y	Y	Verkada Legal Team, Verkada Security Team
A.5.20	Addressing information security within supplier agreements Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Applicable	N	N	Y	Y	Y	Verkada Legal Team, Verkada Security Team
A.5.21	Managing information security in the ICT supply chain Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.22	Monitoring, review and change management of supplier services The organization should regularly monitor, review, evaluate and	Applicable	N	N	Y	Y	Y	Verkada Legal Team, Verkada

	manage change in supplier information security practices and service delivery.								Security Team
A.5.23	Information security for use of cloud services Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.	Applicable	N	N	Y	Y	Y		Verkada Security Team
A.5.24	Information security incident management planning and preparation The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Applicable	N	N	Y	Y	Y		Verkada Security Team
A.5.25	Assessment and decision on information security events The organization should assess information security events and decide if they are to be categorized as information security incidents.	Applicable	N	N	Y	Y	Y		Verkada Security Team



A.5.26	Response to information security incidents Information security incidents should be responded to in accordance with the documented procedures.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.27	Learning from information security incidents Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.28	Collection of evidence The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.29	Information security during disruption The organization should plan how to maintain information security at an appropriate level during disruption.	Applicable	N	N	Y	Y	Y	Verkada Security Team

A.5.30	ICT readiness for business continuity ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.31	Legal, statutory, regulatory and contractual requirements Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.	Applicable	N	N	Y	Y	Y	Verkada Legal Team
A.5.32	Intellectual property rights The organization should implement appropriate procedures to protect intellectual property rights.	Applicable	N	N	Y	Y	Y	Verkada Legal Team
A.5.33	Protection of records Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Applicable	N	N	Y	Y	Y	Verkada Security Team, Verkada Engineering Team

A.5.34	Privacy and protection of PII The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Applicable	N	N	Y	Y	Y	Verkada Privacy Team, Verkada Security Team, Verkada Engineering Team
A.5.35	Independent review of information security The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.	Applicable	N	N	Y	Y	Y	CertPro
A.5.36	Compliance with policies, rules and standards for information security Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.5.37	Documented operating procedures Operating procedures for information processing facilities should be documented and made	Applicable	N	N	Y	Y	Y	Verkada Engineering Team

	available to personnel who need them.							
A.6	PEOPLE CONTROLS							
A.6.1	Screening Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Applicable	N	N	Y	Y	Y	Verkada People Team
A.6.2	Terms and conditions of employment The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	Applicable	N	N	Y	Y	Y	Verkada People Team
A.6.3	Information security awareness, education and training Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and	Applicable	N	N	Y	Y	Y	Verkada People Team, Verkada Security Team

	training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.							
A.6.4	Disciplinary process A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Applicable	N	N	Y	Y	Y	Verkada People Team
A.6.5	Responsibilities after termination or change of employment Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	Applicable	N	N	Y	Y	Y	Verkada
A.6.6	Confidentiality or non-disclosure agreements Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be	Applicable	N	N	Y	Y	Y	Verkada Legal Team, Verkada People Team

	identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.							
A.6.7	Remote working Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team
A.6.8	Information security event reporting The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.7	PHYSICAL CONTROLS							
A.7.1	Physical security perimeters Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Applicable	N	N	Y	Y	Y	Verkada Physical Security Team
A.7.2	Physical entry	Applicable	N	N	Y	Y	Y	Verkada Physical

	Secure areas should be protected by appropriate entry controls and access points.								Security Team
A.7.3	Securing offices, rooms and facilities Physical security for offices, rooms and facilities should be designed and implemented.	Applicable	N	N	Y	Y	Y		Verkada Physical Security Team
A.7.4	Physical security monitoring Premises should be continuously monitored for unauthorized physical access.	Applicable	N	N	Y	Y	Y		Verkada Physical Security Team
A.7.5	Protecting against physical and environmental threats Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	Not Applicable	N	N	N	N	N	Verkada exclusively utilizes cloud infrastructure, opting not to employ on-premises servers for greater scalability and flexibility. This strategic decision alleviates conventional on-premises concerns by transferring responsibility to the cloud provider.	N/A

A.7.6	Working in secure areas Security measures for working in secure areas should be designed and implemented.	Not Applicable	N	N	N	N	N	Verkada exclusively utilizes cloud infrastructure, opting not to employ on-premises servers for greater scalability and flexibility. This strategic decision alleviates conventional on-premises concerns by transferring responsibility to the cloud provider.	N/A
A.7.7	Clear desk and clear screen Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Applicable	N	N	Y	Y	Y		Verkada Security Team
A.7.8	Equipment siting and protection Equipment should be sited securely and protected.	Not Applicable	N	N	N	N	N	Verkada exclusively utilizes cloud infrastructure, opting not to employ on-premises servers for greater	N/A



								scalability and flexibility. This strategic decision alleviates conventional on-premises concerns by transferring responsibility to the cloud provider.	
A.7.9	Security of assets off-premises Off-site assets should be protected.	Applicable	N	N	N	Y	Y	This Annex is scoped to Verkada's employee devices (Endpoint protection, mobile device management, single-sign on, zero-trust network access).	Verkada IT Team
A.7.10	Storage media Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	Applicable	N	N	N	Y	Y	This Annex is scoped to Verkada's employee devices (Endpoint protection, mobile device management).	Verkada IT Team

A.7.11	Supporting utilities Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Not Applicable	N	N	N	N	N	Verkada exclusively utilizes cloud infrastructure, opting not to employ on-premises servers for greater scalability and flexibility. This strategic decision alleviates conventional on-premises concerns by transferring responsibility to the cloud provider.	N/A
A.7.12	Cabling security Cables carrying power, data or supporting information services should be protected from interception, interference or damage.	Not Applicable	N	N	N	N	N	Verkada exclusively utilizes cloud infrastructure, opting not to employ on-premises servers for greater scalability and flexibility. This strategic decision alleviates conventional on-premises concerns by	N/A

								transferring responsibility to the cloud provider.	
A.7.13	Equipment maintenance Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	Applicable	N	N	N	Y	Y	This Annex is scoped to Verkada's employee devices (Endpoint protection, mobile device management).	Verkada IT Team
A.7.14	Secure disposal or re-use of equipment Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Applicable	N	N	N	Y	Y	This Annex is scoped to Verkada's employee devices (Endpoint protection, mobile device management).	Verkada IT Team, Verkada Engineering Team, Verkada Security Team
A.8	TECHNICAL CONTROLS								
A.8.1	User endpoint devices Information stored on, processed by or accessible via user endpoint devices should be protected.	Applicable	N	N	Y	Y	Y		Verkada IT Team
A.8.2	Privileged access rights The allocation and use of privileged access rights should be restricted and managed.	Applicable	N	N	Y	Y	Y		Verkada Security Team

A.8.3	Information access restriction Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team, Verkada IT Team
A.8.4	Access to source code Read and write access to source code, development tools and software libraries should be appropriately managed.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.8.5	Secure authentication Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.8.6	Capacity management The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.7	Protection against malware Protection against malware should be implemented and supported by appropriate user awareness.	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team

A.8.8	Management of technical vulnerabilities Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.8.9	Configuration management Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team
A.8.10	Information deletion Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team, Verkada Security Team
A.8.11	Data masking Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and	Applicable	N	N	Y	Y	Y	Verkada Engineering Team

	business requirements, taking applicable legislation into consideration.							
A.8.12	Data leakage prevention Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Applicable	N	N	Y	Y	Y	Verkada IT Team, Verkada Security Team
A.8.13	Information backup Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.14	Redundancy of information processing facilities Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Applicable	N	N	Y	Y	Y	Redundancy is implemented in Verkada cloud providers, not on-premise. Verkada Engineering Team
A.8.15	Logging Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Applicable	N	N	Y	Y	Y	Verkada Security Team

A.8.16	Monitoring activities Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.8.17	Clock synchronization The clocks of information processing systems used by the organization should be synchronized to approved time sources.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.18	Use of privileged utility programs The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	Applicable	N	N	Y	Y	Y	Verkada IT Team
A.8.19	Installation of software on operational systems Procedures and measures should be implemented to securely manage software installation on operational systems.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team, Verkada IT Team
A.8.20	Networks security Networks and network devices should be secured, managed and	Applicable	N	N	Y	Y	Y	Verkada Security Team

	controlled to protect information in systems and applications.							
A.8.21	Security of network services Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.22	Segregation of networks Groups of information services, users and information systems should be segregated in the organization's networks.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.23	Web filtering Access to external websites should be managed to reduce exposure to malicious content.	Applicable	N	N	Y	Y	Y	Verkada IT Team
A.8.24	Use of cryptography Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	Applicable	N	N	Y	Y	Y	Verkada Security Team
A.8.25	Secure development life cycle Rules for the secure development of software and systems should be established and applied.	Applicable	N	N	Y	Y	Y	Verkada Security Team



A.8.26	Application security requirements Information security requirements should be identified, specified and approved when developing or acquiring applications.	Applicable	N	N	Y	Y	Y	Verkada Security Team, Verkada Engineering Team
A.8.27	Secure system architecture and engineering principles Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	Applicable	N	N	Y	Y	Y	Verkada Security Team, Verkada Engineering Team
A.8.28	Secure coding Secure coding principles should be applied to software development.	Applicable	N	N	Y	Y	Y	Verkada Security Team, Verkada Engineering Team
A.8.29	Security testing in development and acceptance Security testing processes should be defined and implemented in the development life cycle.	Applicable	N	N	Y	Y	Y	Verkada Security Team, Verkada Engineering Team
A.8.30	Outsourced development The organization should direct, monitor and review the activities	Applicable	N	N	Y	Y	Y	Verkada Security Team

	related to outsourced system development.							
A.8.31	Separation of development, test and production environments Development, testing and production environments should be separated and secured.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.32	Change management Changes to information processing facilities and information systems should be subject to change management procedures.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team, Verkada IT Team, Verkada Security Team
A.8.33	Test information Test information should be appropriately selected, protected and managed.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team
A.8.34	Protection of information systems during audit testing Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Applicable	N	N	Y	Y	Y	Verkada Engineering Team, Verkada IT Team, Verkada Security Team



# ISO 27017

CONTROL	OBJECTIVE	DESCRIPTION	STATUS (Applicable/Not Applicable)	IMPLEMENTATION (Yes/No)	Remark
CLD.6.3	Relationship between cloud service customer and cloud service provider				
CLD.6.3.1	Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service are allocated to identified parties, documented, communicated, and implemented.	Applicable	Yes	
CLD.8.1	Responsibility for assets				
CLD.8.1.5	Removal of cloud service customer assets	Cloud Service assets are removed, and returned if necessary, in a timely manner upon the termination of the service agreement	Applicable	Yes	
CLD.9.5	Access control of cloud service customer data in a shared virtual environment				

CLD9.5.1	Segregation in virtual computing environment	The virtual environment is protected from other cloud service customers and unauthorized persons.	Applicable	Yes	
CLD9.5.2	Virtual machine hardening	Virtual machines in the cloud computing environment are hardened to meet business needs.	Applicable	Yes	
CDL12.1	Operational procedures and responsibilities				
CLD12.1.5	Administrator's operational security	Procedures for administrative operations of cloud computing environment are defined, documented, and monitored	Applicable	Yes	
CLD12.4.5	Monitoring of cloud services	Verkada has processes in place to monitor specific aspects of the operation of the cloud services	Applicable	Yes	
CLD13.1	Network security management				

CLD.13.1.4	Alignment of security management for virtual and physical networks	Configurations between virtual and physical networks are verified based on the cloud service provider's network security policy.	Applicable	Yes	
------------	--	--	------------	-----	--

## ISO 27018:2019

CONTROL	OBJECTIVE	DESCRIPTION	STATUS (Applicable/Not Applicable)	IMPLEMENTATION (Yes/No)	Remark
A.2	Consent and choice				
A.2.1	Obligation to cooperate regarding PII principals' rights	Verkda provides the cloud service customer with the means to enable them to fulfill their obligation to facilitate the exercise of PII principals' rights to access, correct, and/or erase PII pertaining to them.	Applicable	Yes	
A.3	Purpose legitimacy and specification				
A.3.1	Public cloud PII processor's purpose	Verkada processes data only for the purpose for which the customer has provided the data and intended use	Applicable	Yes	

A.3.2	Public cloud PII processor's commercial use	Data is not used for marketing and advertising purposes without express consent.	Applicable	Yes	
A.5	Data minimization				
A.5.1	Secure erasure of temporary files	Temporary files and documents are erased or destroyed within a specified, documented period.	Applicable	Yes	
A.6	Use, retention, and disclosure limitation				
A.6.1	PII disclosure notification	Verkada will provide notification to the customer in case of a request for data disclosure as needed	Applicable	Yes	
A.6.2	Recording of PII disclosures	Disclosures of PII to third parties are recorded in the ticketing system, including what PII has been disclosed, to whom, and at what time.	Applicable	Yes	
A.8	Openness, transparency and notice				



A.8.1	Disclosure of sub-contracted PII processing	Verkada will disclose appropriate information about all the sub-contractors used and the scope of personal data processing performed	Applicable	Yes	
A.10	Accountability				
A.10.1	Notification of a data breach involving PII	In the event of a breach, customers will receive a notification of the incident.	Applicable	Yes	
A.10.2	Retention period for administrative security policies and guidelines	Copies of security policies and operating procedures are retained for a specified, documented period upon replacement (including updating).	Applicable	Yes	
A.10.3	PII return, transfer, and disposal	Verkada has an established policy for the return, transfer, and disposal of personal data	Applicable	Yes	
A.11	Information security				

A.11.1	Confidentiality or non-disclosure agreements	Verkada personnel with access to PII sign and agree to a confidentiality agreement	Applicable	Yes	
A.11.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII is restricted	Applicable	Yes	
A.11.3	Control and logging of data restoration	An established procedure for, and a log of, data restoration efforts is in place	Applicable	Yes	
A.11.4	Protecting data on storage media leaving the premises	PII on media leaving Verkada's premises are subject to an authorization procedure and are not accessible to anyone other than authorized personnel	Not Applicable	No	Verkada relies on cloud infrastructure for storing Personally Identifiable Information (PII) and customer data, abstaining from the use of any physical storage media.

A.11.5	Use of unencrypted portable storage media and devices	Verkada restricts the use of media that does not have encryption capability	Not Applicable	No	Verkada relies on cloud infrastructure for storing Personally Identifiable Information (PII) and customer data, abstaining from the use of any physical storage media.
A.11.6	Encryption of PII transmitted over public data-transmission networks	Data transmitted over public networks is encrypted in transit	Applicable	Yes	
A.11.7	Secure disposal of hardcopy materials	Hardcopy materials are destroyed using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	Not Applicable	No	Verkada refrains from generating or gathering hard copies of Personally Identifiable Information (PII)
A.11.8	Unique use of user IDs	Unique user IDs are used within the service	Applicable	Yes	

A.11.9	Records of authorized users	Verkada maintains an up-to-date record of the users or profiles of users who have authorized access to the information system	Applicable	Yes	
A.11.10	User ID management	Usage of expired IDs is not permitted. Unique user IDs are used within the service.	Applicable	Yes	
A.11.11	Contract measures	Minimum security controls are outlined in contracts or agreements with customers and subcontractors	Applicable	Yes	
A.11.12	Sub-contracted PII processing	Minimum security controls are reviewed from appropriate reports from subcontractors that process PII	Applicable	Yes	

A.11.13	Access to data on pre-used data storage space	Deletion of data in storage assigned to other customers (zeroing out of existing data) is performed as needed	Applicable	Yes	
A.12	Privacy compliance				
A.12.1	Geographical location of PII	Verkada will specify and document the countries in which PII might possibly be stored.	Applicable	Yes	
A.12.2	Intended destination of PII	PII transmitted using a data-transmission network are subject to appropriate controls designed to ensure that data reaches its intended destination.	Applicable	Yes	

## Change Log

Version	Date	Author	Summary
1.0	Feb 29, 2024	Kyle Randolph	Initial Version

July 15, 2024



2125 Western Ave.,

Suite 208

Seattle, WA 98121

206-753-7649

<https://www.anvilsecure.com>

To Whom It May Concern,

This letter attests that Anvil Secure, hereby referred to as Anvil, performed a web application penetration test against the Verkada Command web application and its backend APIs. Two Anvil security engineers performed testing and reporting tasks across (15) days from April 9 to 18, 2024.

Prior to conducting the assessment, a kick-off call was scheduled with Verkada to confirm the target scope, as well as discuss testing requirements and dependencies that might be needed to successfully complete the test. The main focus was mutually agreed to be on the new features introduced since the latest application assessment, which were the following: Web Authentication, PassKey Management, Partner Tools, Temporary Users, Incident Management, and Session Management. The Verkada Command web application and APIs were also tested as a whole, but in a time-boxed manner focusing only on likely attack vectors and entry points. The primary objective of this assessment was to identify potential threats in Verkada Command, which could translate to risks that would affect the confidentiality, integrity and availability of the application itself and the customer data it holds.

Anvil performed both manual and automated testing against the targets using a white-box approach. The code of every component was provided to Anvil by Verkada, and was used to validate assumptions about server-side behavior for the different components. Credentials were also provided for accessing a Verkada Command environment with test devices already set up, to ensure better coverage.

As a result, a total of nine (9) findings were identified, including one (1) high-severity, six (6) low-severity, and two (2) informational-severity findings. A remediation test was conducted by an Anvil security engineer between June 26 and June 27, 2024. Of the one (1) high-severity and six (6) low-severity findings, all six (6) low-severity findings were fully remediated, and the high-severity finding was partially remediated.

It is noted that the original high-severity finding has been downgraded to medium-severity, as the majority of targets have been addressed. Verkada has an ongoing project to address the remaining targets. In addition, one of the original informational-severity findings was tied to a few outdated JavaScript dependencies that were identified, which have mostly been addressed by Verkada. There is also an ongoing program to address these issues more proactively in the future.

---

2125 Western Ave., Suite 208, Seattle, WA 98121

July 15, 2024

**ANVIL**

**SECURE**

If there are any further questions pertaining to this document, please do not hesitate to channel any inquiries via Verkada's product and engineering teams who have the means to contact Anvil's Service Delivery team.

Project Manager

thomas.zech@anvilsecure.com

[www.anvilsecure.com](http://www.anvilsecure.com)

Driven Security  
adam@drivenlocks.com

---

2125 Western Ave., Suite 208, Seattle, WA 98121





March 13<sup>th</sup>, 2025

Mr. Kevin Jones  
Johnson Controls Criminal Justice Operations  
1281 Newell Parkway  
Montgomery, AL 36110

Dear Mr. Jones:

Please accept this letter as recognition of Johnson Controls Criminal Justice Operations' nearly 20 years of experience programming, installing, and supporting Omron Automation products (PLC's, relays, etc.) and Omron-InduSoft HMI products in the Security & Detention industry. This letter may serve as a validation of your current status as an Omron-InduSoft Certified System Integrator.

Thank you for your continued support and valuable expertise in applying our products in the detention industry.

Sincerely,

Sam Mader  
Strategic Account Manager - Security and Detention Industry  
Omron Electronics, LLC  
(608) 286-5657



---

June 18<sup>th</sup>, 2020

To Whom It May Concern:

Please accept by this letter that Johnson Controls, USA (JCI) is an authorized dealer of Harding Instruments' MicroComm DXI and DXL digital intercom systems, and is fully qualified to design, install, and support these systems.

Any questions or concerns regarding the above may be addressed to the undersigned.

Sincerely,

A handwritten signature in blue ink, appearing to read "J. Wheeler", with a stylized flourish at the end.

Joseph Wheeler, P. Eng.

President

# Certified Platinum Member

## FY26



Presented to	DRIVEN Security LLC
Date certified	02-01-2025
Expiration Date	07-31-2025

Authorized by

Ryan Bettencourt  
SVP of Global Channel



**EMPLOYMENT ELIGIBILITY VERIFICATION (E-VERIFY) CERTIFICATION**  
(Florida Statutes, Section 448.095)

PROJECT NAME: **Polk County South & Central County Jail Security Upgrades**

The undersigned, as an authorized officer of the contractor identified below (the "**Contractor**"), having full knowledge of the statements contained herein, hereby certifies to Polk County, a political subdivision of the State of Florida (the "**County**"), by and on behalf of the Contractor in accordance with the requirements of Section 448.095, Florida Statutes, as related to the contract entered into by and between the Contractor and the County on or about the date hereof, whereby the Contractor will provide labor, supplies, or services to the County in exchange for salary, wages, or other remuneration (the "**Contract**"), as follows:

1. Unless otherwise defined herein, terms used in this Certification which are defined in Section 448.095, Florida Statutes, as may be amended from time to time, shall have the meaning ascribed in said statute.

2. Pursuant to Section 448.095(5), Florida Statutes, the Contractor, and any subcontractor under the Contract, must register with and use the E-Verify system to verify the work authorization status of all new employees of the Contractor or subcontractor. The Contractor acknowledges and agrees that (i) the County and the Contractor may not enter into the Contract, and the Contractor may not enter into any subcontracts thereunder, unless each party to the Contract, and each party to any subcontracts thereunder, registers with and uses the E-Verify system; and (ii) use of the U.S. Department of Homeland Security's E-Verify System and compliance with all other terms of this Certification and Section 448.095, Fla. Stat., is an express condition of the Contract, and the County may treat a failure to comply as a material breach of the Contract.

3. By entering into the Contract, the Contractor becomes obligated to comply with the provisions of Section 448.095, Fla. Stat., "Employment Eligibility," as amended from time to time. This includes but is not limited to utilization of the E-Verify System to verify the work authorization status of all newly hired employees, and requiring all subcontractors to provide an affidavit attesting that the subcontractor does not employ, contract with, or subcontract with, an unauthorized alien. The Contractor shall maintain a copy of such affidavit for the duration of the Contract. Failure to comply will lead to termination of the Contract, or if a subcontractor knowingly violates the statute or Section 448.09(1), Fla. Stat., the subcontract must be terminated immediately. If the Contract is terminated pursuant to Section 448.095, Fla. Stat., such termination is not a breach of contract and may not be considered as such. Any challenge to termination under this provision must be filed in the Tenth Judicial Circuit Court of Florida no later than 20 calendar days after the date of termination. If the Contract is terminated for a violation of Section 448.095, Fla. Stat., by the Contractor, the Contractor may not be awarded a public contract for a period of 1 year after the date of termination. The Contractor shall be liable for any additional costs incurred by the County as a result of the termination of the Contract. Nothing in this Certification shall be construed to allow intentional discrimination of any class protected by law.

Executed this 28th day of April, 2025.

**ATTEST:**

By: 

PRINTED NAME: Pat Durham

Its: Director of Construction

**CONTRACTOR:**

By: 

PRINTED NAME: Adam Birdwell

Its: Owner

**EMPLOYMENT ELIGIBILITY VERIFICATION (E-VERIFY) CERTIFICATION**

(Florida Statutes, Section 448.095)

PROJECT NAME: **Polk County South & Central County Jail Security Upgrades**

The undersigned, as an authorized officer of the contractor identified below (the "**Contractor**"), having full knowledge of the statements contained herein, hereby certifies to Polk County, a political subdivision of the State of Florida (the "**County**"), by and on behalf of the Contractor in accordance with the requirements of Section 448.095, Florida Statutes, as related to the contract entered into by and between the Contractor and the County on or about the date hereof, whereby the Contractor will provide labor, supplies, or services to the County in exchange for salary, wages, or other remuneration (the "**Contract**"), as follows:

1. Unless otherwise defined herein, terms used in this Certification which are defined in Section 448.095, Florida Statutes, as may be amended from time to time, shall have the meaning ascribed in said statute.

2. Pursuant to Section 448.095(5), Florida Statutes, the Contractor, and any subcontractor under the Contract, must register with and use the E-Verify system to verify the work authorization status of all new employees of the Contractor or subcontractor. The Contractor acknowledges and agrees that (i) the County and the Contractor may not enter into the Contract, and the Contractor may not enter into any subcontracts thereunder, unless each party to the Contract, and each party to any subcontracts thereunder, registers with and uses the E-Verify system; and (ii) use of the U.S. Department of Homeland Security's E-Verify System and compliance with all other terms of this Certification and Section 448.095, Fla. Stat., is an express condition of the Contract, and the County may treat a failure to comply as a material breach of the Contract.

3. By entering into the Contract, the Contractor becomes obligated to comply with the provisions of Section 448.095, Fla. Stat., "Employment Eligibility," as amended from time to time. This includes but is not limited to utilization of the E-Verify System to verify the work authorization status of all newly hired employees, and requiring all subcontractors to provide an affidavit attesting that the subcontractor does not employ, contract with, or subcontract with, an unauthorized alien. The Contractor shall maintain a copy of such affidavit for the duration of the Contract. Failure to comply will lead to termination of the Contract, or if a subcontractor knowingly violates the statute or Section 448.09(1), Fla. Stat., the subcontract must be terminated immediately. If the Contract is terminated pursuant to Section 448.095, Fla. Stat., such termination is not a breach of contract and may not be considered as such. Any challenge to termination under this provision must be filed in the Tenth Judicial Circuit Court of Florida no later than 20 calendar days after the date of termination. If the Contract is terminated for a violation of Section 448.095, Fla. Stat., by the Contractor, the Contractor may not be awarded a public contract for a period of 1 year after the date of termination. The Contractor shall be liable for any additional costs incurred by the County as a result of the termination of the Contract. Nothing in this Certification shall be construed to allow intentional discrimination of any class protected by law.

Executed this 28th day of April, 2025.

**ATTEST:**

By: 

PRINTED NAME: Lory Ann Van Cor

Its: Witness

**CONTRACTOR:**

By: 

PRINTED NAME: Kenneth Lee Sellers

Its: Fire Systems Manager, West Florida

## AFFIDAVIT CERTIFICATION IMMIGRATION LAWS

SOLICITATION NO.: RFP 25-191, Polk County South & Central County Jail Security  
Upgrades

POLK COUNTY WILL NOT INTENTIONALLY AWARD COUNTY CONTRACTS TO ANY CONSULTANT WHO KNOWINGLY EMPLOYS UNAUTHORIZED ALIEN WORKERS, CONSTITUTING A VIOLATION OF THE EMPLOYMENT PROVISIONS CONTAINED IN 8 U.S.C. SECTION 1324 a(e) {SECTION 274A(e) OF THE IMMIGRATION AND NATIONALITY ACT ("INA").

POLK COUNTY MAY CONSIDER THE EMPLOYMENT BY ANY CONSULTANT OF UNAUTHORIZED ALIENS A VIOLATION OF SECTION 274A(e) OF THE INA. **SUCH VIOLATION BY THE RECIPIENT OF THE EMPLOYMENT PROVISIONS CONTAINED IN SECTION 274A(e) OF THE INA SHALL BE GROUNDS FOR UNILATERAL CANCELLATION OF THE CONTRACT BY POLK COUNTY.**

PROPOSER ATTESTS THAT THEY ARE FULLY COMPLIANT WITH ALL APPLICABLE IMMIGRATION LAWS (SPECIFICALLY TO THE 1986 IMMIGRATION ACT AND SUBSEQUENT AMENDMENTS).

Company Name: Johnson Controls Fire Protection LP

Signature: \_\_\_\_\_

Title: Market General Manager

Date: 29th April 2025

State of: FLORIDA

County of: HILLSBOROUGH

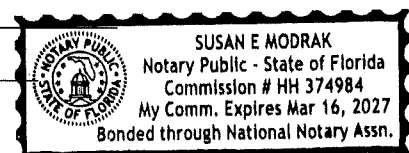
The foregoing instrument was acknowledged before me by means of ☒ physical presence or ☐ online notarization, this 29 day of APRIL, 2025, by Carlos Miller (name) as Market General Manager (title of officer) of Johnson Controls (entity name), on behalf of the company, who ☒ is personally known to me or ☐ has produced \_\_\_\_\_ as identification.

Notary Public Signature: Susan E Modrak

Printed Name of Notary Public: \_\_\_\_\_

Notary Commission Number and Expiration: \_\_\_\_\_

(AFFIX NOTARY SEAL)





## AFFIDAVIT CERTIFICATION IMMIGRATION LAWS

SOLICITATION NO.: **RFP 25-191, Polk County South & Central County Jail Security Upgrades**

POLK COUNTY WILL NOT INTENTIONALLY AWARD COUNTY CONTRACTS TO ANY CONSULTANT WHO KNOWINGLY EMPLOYS UNAUTHORIZED ALIEN WORKERS, CONSTITUTING A VIOLATION OF THE EMPLOYMENT PROVISIONS CONTAINED IN 8 U.S.C. SECTION 1324 a(e) {SECTION 274A(e) OF THE IMMIGRATION AND NATIONALITY ACT ("INA").

POLK COUNTY MAY CONSIDER THE EMPLOYMENT BY ANY CONSULTANT OF UNAUTHORIZED ALIENS A VIOLATION OF SECTION 274A(e) OF THE INA. **SUCH VIOLATION BY THE RECIPIENT OF THE EMPLOYMENT PROVISIONS CONTAINED IN SECTION 274A(e) OF THE INA SHALL BE GROUNDS FOR UNILATERAL CANCELLATION OF THE CONTRACT BY POLK COUNTY.**

PROPOSER ATTESTS THAT THEY ARE FULLY COMPLIANT WITH ALL APPLICABLE IMMIGRATION LAWS (SPECIFICALLY TO THE 1986 IMMIGRATION ACT AND SUBSEQUENT AMENDMENTS).

Company Name: Driven Security LLC

Signature: [Signature]

Title: Owner

Date: 4/28/25

State of: TN

County of: Rutherford

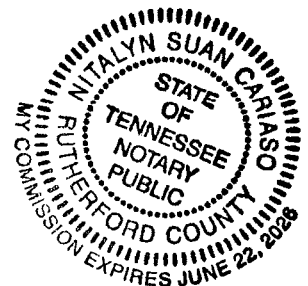
The foregoing instrument was acknowledged before me by means of ☒ physical presence or ☐ online notarization, this 28<sup>th</sup> day of APRIL, 2025, by ADAM BIROWELL (name) as OWNER (title of officer) of DRIVEN SECURITY (entity name), on behalf of the company, who ☒ is personally known to me or ☐ has produced \_\_\_\_\_ as identification.

Notary Public Signature: [Signature]

Printed Name of Notary Public: Nitalyn Swan Cariaso

Notary Commission Number and Expiration: 6.22.24

(AFFIX NOTARY SEAL)



## Drug-Free Workplace Form

(Submittal Page)

The undersigned vendor in accordance with Florida Statue 287.087 hereby certifies that, (Name of the Business): Driven Security LLC does:

1. Publish a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the actions that will be taken against employees for violations of such prohibition.
2. Inform employees about the dangers of drug abuse in the workplace, the business's policy of maintaining a drug-free workplace, any available drug counseling, rehabilitation programs, employee assistance programs and the penalties that may be imposed upon employees for drug abuse violations.
3. Give each employee engaged in providing the commodities or contractual services that are under this RFP a copy of the statement specified in subsection (1).
4. In the statement specified in subsection (1), notify the employees that, as a condition of working on the commodities or contractual services that are under this RFP, the employee will abide by the terms of the statement and will notify the employer of any conviction of, plea of guilty or nolo contendere to, any violation of Chapter 1893 or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction.
5. Impose a sanction on or require the satisfactory participation in a drug abuse assistance or rehabilitation program, if such is available in the employee's community, by any employee who is so convicted.
6. Make a good faith effort to continue to maintain a drug-free workplace through implementation of this section.

As the person authorized to sign the statement, I certify that this firm complies fully with the above requirements.

Vendor Signature: 

Date: 4/15/25



## Drug-Free Workplace Form

(Submittal Page)

The undersigned vendor in accordance with Florida Statue 287.087 hereby certifies that, (Name of the Business): Johnson Controls Fire Protection LP does:

1. Publish a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the actions that will be taken against employees for violations of such prohibition.
2. Inform employees about the dangers of drug abuse in the workplace, the business's policy of maintaining a drug-free workplace, any available drug counseling, rehabilitation programs, employee assistance programs and the penalties that may be imposed upon employees for drug abuse violations.
3. Give each employee engaged in providing the commodities or contractual services that are under this RFP a copy of the statement specified in subsection (1).
4. In the statement specified in subsection (1), notify the employees that, as a condition of working on the commodities or contractual services that are under this RFP, the employee will abide by the terms of the statement and will notify the employer of any conviction of, plea of guilty or nolo contendere to, any violation of Chapter 1893 or of any controlled substance law of the United States or any state, for a violation occurring in the workplace no later than five (5) days after such conviction.
5. Impose a sanction on or require the satisfactory participation in a drug abuse assistance or rehabilitation program, if such is available in the employee's community, by any employee who is so convicted.
6. Make a good faith effort to continue to maintain a drug-free workplace through implementation of this section.

As the person authorized to sign the statement, I certify that this firm complies fully with the above requirements.

Vendor Signature: \_\_\_\_\_

Date: 4/29/25

## Proposers Incorporation Information

(Submittal Page)

The following section should be completed by all bidders and submitted with their bid submittal:

Company Name: Johnson Controls Fire Protection LP

DBA/Fictitious Name (if applicable): \_\_\_\_\_

TIN #: 82-4176107

Address: 3802 Sugar Palm Drive

City: Tampa

State: Florida

Zip Code: 33619

County: Hillsborough

Note: Company name must match legal name assigned to the TIN number. A current W9 should be submitted with your bid submittal.

Contact Person: Frank Reinhart

Phone Number: \_\_\_\_\_

Cell Phone Number: 813-310-9770

Email Address: frank.reinhart@jci.com

Type of Organization (select one type)

- ☐ Sole Proprietorship
- ☐ Partnership
- ☐ Non-Profit
- ☐ Sub Chapter
- ☐ Joint Venture
- ☒ Corporation
- ☐ LLC
- ☒ LLP
- ☐ Publicly Traded
- ☐ Employee Owned

State of Incorporation: Wisconsin

The Successful vendor must complete and submit this form prior to award. The Successful vendor must invoice using the company name listed above.

**Request for Taxpayer  
Identification Number and Certification**

Go to [www.irs.gov/FormW9](http://www.irs.gov/FormW9) for instructions and the latest information.

**Give form to the  
requester. Do not  
send to the IRS.**

**Before you begin.** For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See Specific Instructions on page 3.	<b>1</b> Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.) <b>JOHNSON CONTROLS US HOLDINGS INC</b>	<b>4</b> Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):  Exempt payee code (if any) <b>5</b>  Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any) <b>E</b>  (Applies to accounts maintained outside the United States.)
	<b>2</b> Business name/disregarded entity name, if different from above. <b>JOHNSON CONTROLS FIRE PROTECTION LP (FEIN 58-2608861, FKA SimplexGrinnell LP)</b>	
	<b>3a</b> Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only <b>one</b> of the following seven boxes. <input type="checkbox"/> Individual/sole proprietor <input checked="" type="checkbox"/> C corporation <input type="checkbox"/> S corporation <input type="checkbox"/> Partnership <input type="checkbox"/> Trust/estate <input type="checkbox"/> LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) _____ <b>Note:</b> Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner. <input type="checkbox"/> Other (see instructions) _____	
	<b>3b</b> If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions _____ <input type="checkbox"/>	
	<b>5</b> Address (number, street, and apt. or suite no.). See instructions. <b>5757 N Green Bay Ave</b>	
<b>6</b> City, state, and ZIP code <b>Milwaukee WI 53209</b>		
<b>7</b> List account number(s) here (optional)		

**Part I Taxpayer Identification Number (TIN)**

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

**Note:** If the account is in more than one name, see the instructions for line 1. See also *What Name and Number To Give the Requester* for guidelines on whose number to enter.

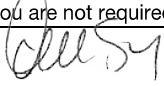
<b>Social security number</b>									
			-				-		
<b>or</b>									
<b>Employer identification number</b>									
8	2		-	4	1	7	6	1	0

**Part II Certification**

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

**Certification instructions.** You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

<b>Sign Here</b>	Signature of U.S. person 	Date <b>1/2/2025</b>
------------------	---	-------------------------

**General Instructions**

Section references are to the Internal Revenue Code unless otherwise noted.

**Future developments.** For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to [www.irs.gov/FormW9](http://www.irs.gov/FormW9).

**What's New**

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

**Purpose of Form**

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they

October 14, 2022

**Re: Clarification of Johnson Controls Fire Protection LP's W-9**

Dear Sir/Madam:

We provide this letter to address any confusion around the W-9 submitted Johnson Controls Fire Protection LP. This is the entity with whom you have contracted, the entity providing products and services to you, and the entity billing you.

However, you may have noticed that the W-9 lists the name of Johnson Controls US Holdings Inc in Line 1. It also lists the FEIN of Johnson Controls US Holdings Inc in Part 1. The reason for this is below.

Johnson Controls Fire Protection LP is a limited partnership that is owned by multiple single-member LLCs that are all disregarded for income tax purposes. As such, the IRS treats Johnson Controls Fire Protection LP as a disregarded entity (in other words, a division of its corporate parent company) for income tax purposes. Because of this, **the IRS requires that we state on ALL W-9 forms the name and FEIN of our corporate parent that actually files the federal tax return.**

The language below is taken directly from the IRS website. As you can see, we are required by IRS rules to provide our corporate parent's FEIN and cannot issue a W-9 with the FEIN of Johnson Controls Fire Protection LP in Part 1. Nor can we list the name Johnson Controls Fire Protection LP in Line 1, despite the fact that this is the legal entity with whom you are dealing.

**Taxpayer Identification Number**

- For federal income tax purposes, a single-member LLC classified as a disregarded entity generally must use the owner's social security number (SSN) or EIN for all information returns and reporting related to income tax. For example, if a disregarded entity LLC that is owned by an individual is required to provide a Form W-9, Request for Taxpayer Identification Number and Certification, the W-9 should provide the owner's SSN or EIN, not the LLC's EIN.

*Source: [www.irs.gov](http://www.irs.gov)*

Johnson Controls Fire Protection LP is listed on the second line (as directed by the IRS). For cross-reference purposes within your AP systems, we have also listed Johnson Controls Fire Protection LP's FEIN (58-2608861) on line 2 of the W-9.

**EFFECT OF THE W-9**

Since the parent entity of Johnson Controls Fire Protection LP is a valid (SubChapter C) corporation, the W-9 certification operates to justify your reporting treatment as follows:

1. Payments made to Johnson Controls Fire Protection LP are NOT subject to 1099 reporting;
2. Payments made to Johnson Controls Fire Protection LP are NOT subject to IRS Back-Up Withholding; and
3. Payments made to Johnson Controls Fire Protection LP are NOT subject to FATCA reporting.

Please note that the address listed on the W-9 represents the formal location of our organization's books and records. However, this W-9 certification applies equally to ALL operational addresses/offices maintained by Johnson Controls Fire Protection LP.

If you have further questions, please consult your tax team.

**2005 LIMITED PARTNERSHIP ANNUAL REPORT**  
**Due By May 1, 2005**

**FILED**  
 05 APR -6 PM 1:19  
 SECRETARY OF STATE  
 TALLAHASSEE, FLORIDA

<b>DOCUMENT # B01000000134</b> 1. Entity Name <b>SIMPLEXGRINNELL LP</b>			
Principal Place of Business <b>100 SIMPLEX DRIVE                  WESTMINSTER, MA 01441</b>		Mailing Address <b>PO BOX 8749                  PRINCETON, NJ 08543</b>	
2. Principal Place of Business <b>One Town Center Road</b> Suite, Apt. #, etc.		3. Mailing Address <b>One Town Center Road</b> Suite, Apt. #, etc.	
City & State <b>Boca Raton, FL</b> Zip <b>33486</b>		City & State <b>Boca Raton, FL</b> Zip <b>33486</b>	
Country		Country	
4. FEI Number <b>58-2608861</b>		Applied For <input type="checkbox"/> Not Applicable	
5. Certificate of Status Desired <input checked="" type="checkbox"/>		<b>\$8.75</b> Additional Fee Required	
6. Name and Address of Current Registered Agent <b>C T CORPORATION SYSTEM                  1200 SOUTH PINE ISLAND ROAD                  PLANTATION, FL 33324</b>		7. Name and Address of New Registered Agent Name Street Address (P.O. Box Number is Not Acceptable) City FL Zip Code	
8. The above named entity submits this statement for the purpose of changing its registered office or registered agent, or both, in the State of Florida. I am familiar with, and accept the obligations of registered agent.			
SIGNATURE _____ DATE _____ <small>Signature, typed or printed name of registered agent and title if applicable.</small>			
9. Capital Contributions as Shown on record. <b>\$57,305,806.00</b>		10. Amount of Capital Contributions in FLORIDA to date. <b>\$57,305,806.</b>	
<b>A GENERAL PARTNER THAT IS A BUSINESS ENTITY MUST BE REGISTERED AND ACTIVE WITH THIS OFFICE.</b> <b>NOTE: General Partners MAY NOT be changed on the form; an amendment must be filed to change a general partner.</b>			
<b>12. GENERAL PARTNER INFORMATION</b>		<b>13. ADDRESS CHANGES ONLY</b>	
DOCUMENT # NAME STREET ADDRESS CITY-ST-ZIP	<b>F01000001903                  STR GRINNELL GP HOLDING, INC.                  100 SIMPLEX DRIVE                  WESTMINSTER, MA 01441</b>	STREET ADDRESS CITY-ST-ZIP	<b>One Town Center Road                  Boca Raton, FL 33486</b>
DOCUMENT # NAME STREET ADDRESS CITY-ST-ZIP		STREET ADDRESS CITY-ST-ZIP	
DOCUMENT # NAME STREET ADDRESS CITY-ST-ZIP		STREET ADDRESS CITY-ST-ZIP	<b>300050821093                  04/15/05--01007--009 **526.25</b>
DOCUMENT # NAME STREET ADDRESS CITY-ST-ZIP		STREET ADDRESS CITY-ST-ZIP	<b>300050821093                  04/15/05--01007--010 **8.75</b>
DOCUMENT # NAME STREET ADDRESS CITY-ST-ZIP		STREET ADDRESS CITY-ST-ZIP	
DOCUMENT # NAME STREET ADDRESS CITY-ST-ZIP		STREET ADDRESS CITY-ST-ZIP	
14. I hereby certify that the information supplied with this filing does not qualify for the exemption stated in Section 119.07(3)(i), Florida Statutes. I further certify that the information indicated on this report is true and accurate and that my signature shall have the same legal effect as if made under oath; that I am a General Partner of the limited partnership or the receiver or trustee empowered to execute this report as required by Chapter 620, Florida Statutes.			
SIGNATURE: <u>Barbara Burke</u>		Vice Pres./Asst. Treas. <u>4-405</u> POA	
<small>SIGNATURE AND TYPED OR PRINTED NAME OF SIGNING GENERAL PARTNER</small>		<small>Date Daytime Phone #</small>	

STAPLE CHECK HERE

## Proposers Incorporation Information

(Submittal Page)

The following section should be completed by all bidders and submitted with their bid submittal:

Company Name: Driven Security LLC

DBA/Fictitious Name (if applicable): NA

TIN #: 81-3198484

Address: 241 Wilson Pike Circle

City: Brentwood

State: TN

Zip Code: 37027

County: Williamson

Note: Company name must match legal name assigned to the TIN number. A current W9 should be submitted with your bid submittal.

Contact Person: Adam Birdwell

Phone Number: 615-490-8664

Cell Phone Number: 615-533-4503

Email Address: adam@drivenlocks.com

Type of Organization (select one type)

- ☐ Sole Proprietorship
- ☐ Partnership
- ☐ Non-Profit
- ☐ Sub Chapter
- ☐ Joint Venture
- ☐ Corporation
- ☒ LLC
- ☐ LLP
- ☐ Publicly Traded
- ☐ Employee Owned

State of Incorporation: TN

The Successful vendor must complete and submit this form prior to award. The Successful vendor must invoice using the company name listed above.

**Request for Taxpayer  
Identification Number and Certification**

Go to [www.irs.gov/FormW9](http://www.irs.gov/FormW9) for instructions and the latest information.

**Give form to the  
requester. Do not  
send to the IRS.**

**Before you begin.** For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See Specific Instructions on page 3.	<b>1</b> Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)	
	<b>Driven Security</b>	
	<b>2</b> Business name/disregarded entity name, if different from above.	
	<b>3a</b> Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only <b>one</b> of the following seven boxes.  <input type="checkbox"/> Individual/sole proprietor <input type="checkbox"/> C corporation <input type="checkbox"/> S corporation <input type="checkbox"/> Partnership <input type="checkbox"/> Trust/estate <input checked="" type="checkbox"/> <b>LLC.</b> Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) . . . . . <b>P</b> <b>Note:</b> Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.  <input type="checkbox"/> Other (see instructions) _____	
	<b>4</b> Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):  Exempt payee code (if any) _____  Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any) _____  (Applies to accounts maintained outside the United States.)	
	<b>3b</b> If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions . . . . . <input type="checkbox"/>	
<b>5</b> Address (number, street, and apt. or suite no.). See instructions. <b>241 Wilson Pike Cir</b>		
<b>6</b> City, state, and ZIP code <b>Brentwood, TN 37027</b>		
<b>7</b> List account number(s) here (optional)		
Requester's name and address (optional)		

<b>Part I Taxpayer Identification Number (TIN)</b>																						
Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see <i>How to get a TIN</i> , later.																						
<b>Social security number</b> <table><tr><td></td><td></td><td></td><td>-</td><td></td><td></td><td>-</td><td></td><td></td><td></td><td></td><td></td></tr></table> <b>or</b> <b>Employer identification number</b> <table><tr><td>8</td><td>1</td><td>-</td><td>3</td><td>1</td><td>9</td><td>8</td><td>4</td><td>8</td><td>4</td></tr></table>				-			-						8	1	-	3	1	9	8	4	8	4
			-			-																
8	1	-	3	1	9	8	4	8	4													
<b>Note:</b> If the account is in more than one name, see the instructions for line 1. See also <i>What Name and Number To Give the Requester</i> for guidelines on whose number to enter.																						

<b>Part II Certification</b>
Under penalties of perjury, I certify that:
1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.
<b>Certification instructions.</b> You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.
<b>Sign Here</b>
Signature of U.S. person <i>Jonathan Pope</i>
Date April 23, 2025

**General Instructions**

Section references are to the Internal Revenue Code unless otherwise noted.

**Future developments.** For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to [www.irs.gov/FormW9](http://www.irs.gov/FormW9).

**What's New**

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

**Purpose of Form**

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)  
04/30/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> MARSH USA LLC 155 N WACKER, SUITE 1200 Chicago, IL 60661 Attn: JCI Certrequest@marsh.com	<b>CONTACT NAME</b> Marsh   U S Operations	<b>FAX (A/C, No):</b>	
	<b>PHONE (A/C, No, Ext):</b> (866) 966-4664	<b>E-MAIL ADDRESS:</b> JCI certrequest@marsh.com	
<b>INSURED</b> Johnson Controls US Holdings, Inc. Johnson Controls, Inc. Johnson Controls Fire Protection LP Johnson Controls Security Solutions LLC (See attached Acord 101) 5757 North Green Bay Avenue Milwaukee, WI 53209	<b>INSURER(S) AFFORDING COVERAGE</b>		<b>NAIC #</b>
	<b>INSURER A:</b> Old Republic Insurance Company		24147
	<b>INSURER B:</b>		
	<b>INSURER C:</b>		
	<b>INSURER D:</b>		
	<b>INSURER E:</b>		
<b>INSURER F:</b>			

**COVERAGES** **CERTIFICATE NUMBER:** CHI-010928882-01 **REVISION NUMBER:** 2

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSD WYD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> Contractual Liability <input checked="" type="checkbox"/> XCU Included GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER		MWZY 313947-24	10/01/2024	10/01/2025	EACH OCCURRENCE \$ 5,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 5,000,000 MED EXP (Any one person) \$ 50,000 PERSONAL & ADV INJURY \$ 5,000,000 GENERAL AGGREGATE \$ 20,000,000 PRODUCTS - COMP/OP AGG \$ INC IN GEN AGG
A	<input checked="" type="checkbox"/> <b>AUTOMOBILE LIABILITY</b> <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> NON-OWNED AUTOS ONLY		MWTB 313946-24 (Excludes New Hamp) MWTB 313949-24 (Primary NH \$250k) MWZX 313950-24 (Excess NH \$4 75mm) Excess NH Auto is Follow Form to Primary NH Auto	10/01/2024 10/01/2024 10/01/2024	10/01/2025 10/01/2025 10/01/2025	COMBINED SINGLE LIMIT (Ea accident) \$ 5,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
	<input type="checkbox"/> <b>UMBRELLA LIAB</b> <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> DED <input type="checkbox"/> RETENTION \$	<input type="checkbox"/> OCCUR <input type="checkbox"/> CLAIMS-MADE				EACH OCCURRENCE \$ AGGREGATE \$
A	<input checked="" type="checkbox"/> <b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	<input type="checkbox"/> Y <input checked="" type="checkbox"/> N	MWC 313943-24 (AOS - see page 2) MWXS 313944-24 (OH & WA)	10/01/2024 10/01/2024	10/01/2025 10/01/2025	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E L EACH ACCIDENT \$ 1,000,000 E L DISEASE - EA EMPLOYEE \$ 1,000,000 E L DISEASE - POLICY LIMIT \$ 1,000,000

**DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES** (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)  
See attached Acord 101 for additional information including Additional Insured, Primary/Non-contributory, Waiver of Subrogation and Notice of Cancellation provisions.

## CERTIFICATE HOLDER

Central County Jail  
2390 Bob Phillips Rd  
Bartow, FL 33830

## CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE  
of Marsh USA LLC

*Paul Mammella*

© 1988-2016 ACORD CORPORATION. All rights reserved.





# **ADDITIONAL REMARKS SCHEDULE**

Page 2 of 2

AGENCY MARSH USA LLC.		NAMED INSURED Johnson Controls US Holdings, Inc. Johnson Controls, Inc. Johnson Controls Fire Protection LP Johnson Controls Security Solutions LLC (See attached Acord 101) 5757 North Green Bay Avenue Milwaukee, WI 53209
POLICY NUMBER		
CARRIER	NAIC CODE	
EFFECTIVE DATE:		

## **ADDITIONAL REMARKS**

**THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,**

**FORM NUMBER:** 25 **FORM TITLE:** Certificate of Liability Insurance

### **WORKERS COMPENSATION:**

Workers Compensation "AOS" Policy includes coverage for employees from the following States WHILE WORKING IN ANY STATE: AK, AL, AR, AZ, CA, CO, CT, DC, DE, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MA, MD, ME, MI, MN, MO, MS, MT, NC, NE, NH, NJ, NM, NV, NY, OK, OR, PA, RI, SC, SD, TN, TX, UT, VA, VT, WI, & WV.

### **PRIMARY COVERAGE:**

The General Liability and Automobile Liability policies are primary and not excess of or contributing with other insurance or self-insurance, where required by written lease or written contract. For General Liability, this applies to both ongoing and completed operations.

### **WAIVER OF SUBROGATION:**

The General Liability, Automobile Liability, Workers' Compensation and Employers Liability policies include a Waiver of Subrogation in favor of the certholder and any other person or organization, BUT ONLY to the extent required by written contract.

### **ADDITIONAL INSURED - AUTOMOBILE LIABILITY:**

The Automobile Liability policy, if required by written contract, includes coverage for Additional Insureds as required by such written contract.

### **ADDITIONAL INSURED - GENERAL LIABILITY:**

For General Liability, if required by written contract, the following are included as additional insureds, as required pursuant to a written contract with a named insured, per attached Policy Endorsements A2 and A2A: THE CERTIFICATE HOLDER LISTED ON THIS CERTIFICATE OF LIABILITY INSURANCE, AND EACH OTHER PERSON OR ORGANIZATION REQUIRED TO BE INCLUDED AS AN ADDITIONAL INSURED PURSUANT TO A WRITTEN CONTRACT WITH THE NAMED INSURED

### **ONGOING OPERATIONS AND COMPLETED OPERATIONS INSURANCE**

The General Liability Insurance includes insurance for ongoing operations and completed operations.

### **LIMIT OF LIABILITY:**

The Liability Limit that applies is the amount indicated on the face of this Certificate of Liability Insurance, or the minimum Liability limit that is required by the written contract, whichever is less. If there is no contract then the Liability Limit is limited to \$1,000,000.

### **NOTICE OF CANCELLATION TO CERTIFICATE HOLDERS:**

Should any of the above described policies be cancelled, other than for non-payment, before the expiration date thereof, 30 days advice of cancellation will be delivered to certificate holders in accordance with the policy endorsements.

### **NAMED INSURED:**

American Chiller Mechanical Service LLC; ArkLaTex Mechanical Services; Central Sprinkler LLC; Chemguard, Inc.; Connect 24 Wireless Communications Inc.; Exacq Technologies, Inc.; FM Systems Europe Limited; FM Systems Group LLC; Grinnell LLC; Haz-Tank Fabricators, Inc.; Integrated Systems and Power, Inc.; IonicBlue Partners LLC; JC Residential and Light Commercial LLC; Johnson Controls (Suisse) SA; Johnson Controls Air Conditioning and Refrigeration, Inc.; Johnson Controls Building Automation Systems, LLC; Johnson Controls Building Solutions LLC; Johnson Controls Capital LLC; Johnson Controls Federal Systems, LLC; Johnson Controls Fire Protection LP; Johnson Controls Foundation, Inc.; Johnson Controls Government Systems, LLC; Johnson Controls, Inc.; Johnson Controls Navy Systems, LLC; Johnson Controls North America Products, LLC; Johnson Controls PI Project Site Operations LLC; Johnson Controls Security Solutions LLC; Johnson Controls-Hitachi Air Conditioning North America LLC; Johnson Controls US Holdings, LLC; M&M Refrigeration, LLC; Master Protection, LP dba FireMaster; Qolsys, Inc.; Rescue Air Systems; Retail Expert, Inc.; Richmond Alarm Company LLC; Security Enhancement Systems LLC; Sensormatic Electronics, LLC; Sensormatic USA LLC; ShopperTrak International Investment LLC; ShopperTrak RCT Corporation; Shurjoint America, Inc.; Silent-Aire USA Inc.; Silent-Aire Mission Critical Service LLC; Tyco Fire & Security LLC; Tyco Fire Products LP; Visonic Inc.; WillFire HC, LLC; York International (SA), Inc.; York International Corporation

# IL 10 (12/06) OLD REPUBLIC INSURANCE COMPANY

## ADDITIONAL INSURED - OWNERS, LESSEES OR CONTRACTORS - SCHEDULED PERSON OR ORGANIZATION - ENDORSEMENT A2

Named Insured Johnson Controls US Holdings, Inc.			Endorsement Number
Policy Prefix	Policy Number MWZY 313947 24	Policy Period 10/01/24 - 10/01/25	Effective Date of Endorsement 10/01/24
Issued By Old Republic Insurance Company			

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

### COMMERCIAL GENERAL LIABILITY COVERAGE PART

### SCHEDULE

#### Name Of Additional Insured Person(s) Or Organization(s):

If required by contract, the person or organization listed on the certificate of insurance as additional insured, and each other person or organization required to be included as an additional insured pursuant to a contract with a named insured.

#### Location(s) Of Covered Operations:

As required by contract.

Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

**A. Section II - Who Is An Insured** is amended to include as an additional insured the person(s) or organization(s) shown in the Schedule, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" caused solely by:

1. Your acts or omissions; or
2. The acts or omissions of those acting on your behalf;

in the performance of your ongoing operations for the additional insured(s) at the location(s) designated above.

**B. With respect to the insurance afforded to these additional insureds, the following additional exclusions apply:**

This insurance does not apply to "bodily injury" or "property damage" occurring after:

1. All work, including materials, parts or equipment furnished in connection with such work, on the project (other than service, maintenance or repairs) to be performed by or on behalf of the additional insured(s) at the location of the covered operations has been completed; or
2. That portion of "your work" out of which the injury or damage arises has been put to its intended use by any person or organization other than another contractor or subcontractor engaged in performing operations for a principal as a part of the same project.

GL 289 001 1012

## IL 10 (12/06) OLD REPUBLIC INSURANCE COMPANY

### ADDITIONAL INSURED - OWNERS, LESSEES OR CONTRACTORS - COMPLETED OPERATIONS - ENDORSEMENT A2A

Named Insured Johnson Controls US Holdings, Inc.			Endorsement Number
Policy Prefix	Policy Number MWZY 313947 24	Policy Period 10/01/24 - 10/01/25	Effective Date of Endorsement 10/01/24
Issued By Old Republic Insurance Company			

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

#### COMMERCIAL GENERAL LIABILITY COVERAGE PART

#### SCHEDULE

##### Name Of Additional Insured Person(s) Or Organization(s):

If required by contract, the person or organization listed on the certificate of insurance as additional insured, and each other person or organization required to be included as an additional insured pursuant to a contract with a named insured.

##### Location And Description Of Completed Operations:

As required by contract.

Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

**Section II - Who Is An Insured** is amended to include as an additional insured the person(s) or organization(s) shown in the Schedule, but only with respect to liability for "bodily injury" or "property damage" caused solely by "your work" at the location designated and described in the Schedule of this endorsement performed for that additional insured and included in the "products-completed operations hazard".

GL 289 002 1012



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)  
04/30/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> MARSH USA LLC 155 N WACKER, SUITE 1200 Chicago, IL 60661 Attn: JCI Certrequest@marsh.com  CN101230596-5-24-25*	<b>CONTACT</b> NAME: Marsh   U S Operations PHONE (A/C, No, Ext): (866) 966-4664 E-MAIL: JCI certrequest@marsh.com ADDRESS:  <b>INSURER(S) AFFORDING COVERAGE</b> INSURER A: Old Republic Insurance Company INSURER B: INSURER C: INSURER D: INSURER E: INSURER F:	<b>FAX (A/C, No):</b>  <b>NAIC #</b> 24147
--	--	---

## COVERAGES

CERTIFICATE NUMBER:

CHI-010928911-01

REVISION NUMBER: 3

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSD WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> Contractual Liability <input checked="" type="checkbox"/> XCU Included GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER		MWZY 313947-24	10/01/2024	10/01/2025	EACH OCCURRENCE \$ 5,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 5,000,000 MED EXP (Any one person) \$ 50,000 PERSONAL & ADV INJURY \$ 5,000,000 GENERAL AGGREGATE \$ 20,000,000 PRODUCTS - COMP/OP AGG \$ INC IN GEN AGG
A	<b>AUTOMOBILE LIABILITY</b> <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY		MWTB 313946-24 (Excludes New Hamp) MWTB 313949-24 (Primary NH \$250k) MWZX 313950-24 (Excess NH \$4.75mm) Excess NH Auto is Follow Form to Primary NH Auto	10/01/2024 10/01/2024 10/01/2024	10/01/2025 10/01/2025 10/01/2025	COMBINED SINGLE LIMIT (Ea accident) \$ 5,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
	<b>UMBRELLA LIAB</b> <input type="checkbox"/> OCCUR <b>EXCESS LIAB</b> <input type="checkbox"/> CLAIMS-MADE DED <input type="checkbox"/> RETENTION \$					EACH OCCURRENCE \$ AGGREGATE \$
A	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N <input checked="" type="checkbox"/> N <input type="checkbox"/> A	MWC 313943-24 (AOS - see page 2) MWXS 313944-24 (OH & WA)	10/01/2024 10/01/2024	10/01/2025 10/01/2025	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E L EACH ACCIDENT \$ 1,000,000 E L DISEASE - EA EMPLOYEE \$ 1,000,000 E L DISEASE - POLICY LIMIT \$ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

See attached Acord 101 for additional information including Additional Insured, Primary/Non-contributory, Waiver of Subrogation and Notice of Cancellation provisions.

## CERTIFICATE HOLDER

South County Jail  
1103 US-98  
Frostproof, FL 33843

## CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE  
of Marsh USA LLC

*Paul Mammella*

AGENCY CUSTOMER ID: CN101230596

LOC #: Milwaukee



# **ADDITIONAL REMARKS SCHEDULE**

Page 2 of 2

AGENCY MARSH USA LLC.		NAMED INSURED Johnson Controls US Holdings, Inc. Johnson Controls, Inc. Johnson Controls Fire Protection LP Johnson Controls Security Solutions LLC (See attached Acord 101) 5757 North Green Bay Avenue Milwaukee, WI 53209	
POLICY NUMBER		EFFECTIVE DATE	
CARRIER	NAIC CODE		

## **ADDITIONAL REMARKS**

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,  
FORM NUMBER: 25 FORM TITLE: Certificate of Liability Insurance

### **WORKERS COMPENSATION:**

Workers Compensation "AOS" Policy includes coverage for employees from the following States WHILE WORKING IN ANY STATE: AK, AL, AR, AZ, CA, CO, CT, DC, DE, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MA, MD, ME, MI, MN, MO, MS, MT, NC, NE, NH, NJ, NM, NV, NY, OK, OR, PA, RI, SC, SD, TN, TX, UT, VA, VT, WI, & WV.

### **PRIMARY COVERAGE:**

The General Liability and Automobile Liability policies are primary and not excess of or contributing with other insurance or self-insurance, where required by written lease or written contract. For General Liability, this applies to both ongoing and completed operations.

### **WAIVER OF SUBROGATION:**

The General Liability, Automobile Liability, Workers' Compensation and Employers Liability policies include a Waiver of Subrogation in favor of the certholder and any other person or organization, BUT ONLY to the extent required by written contract.

### **ADDITIONAL INSURED - AUTOMOBILE LIABILITY:**

The Automobile Liability policy, if required by written contract, includes coverage for Additional Insureds as required by such written contract.

### **ADDITIONAL INSURED - GENERAL LIABILITY:**

For General Liability, if required by written contract, the following are included as additional insureds, as required pursuant to a written contract with a named insured, per attached Policy Endorsements A2 and A2A: THE CERTIFICATE HOLDER LISTED ON THIS CERTIFICATE OF LIABILITY INSURANCE, AND EACH OTHER PERSON OR ORGANIZATION REQUIRED TO BE INCLUDED AS AN ADDITIONAL INSURED PURSUANT TO A WRITTEN CONTRACT WITH THE NAMED INSURED.

### **ONGOING OPERATIONS AND COMPLETED OPERATIONS INSURANCE**

The General Liability Insurance includes insurance for ongoing operations and completed operations.

### **LIMIT OF LIABILITY:**

The Liability Limit that applies is the amount indicated on the face of this Certificate of Liability Insurance, or the minimum Liability limit that is required by the written contract, whichever is less. If there is no contract then the Liability Limit is limited to \$1,000,000.

### **NOTICE OF CANCELLATION TO CERTIFICATE HOLDERS:**

Should any of the above described policies be cancelled, other than for non-payment, before the expiration date thereof, 30 days advice of cancellation will be delivered to certificate holders in accordance with the policy endorsements.

### **NAMED INSURED:**

American Chiller Mechanical Service LLC; ArkLaTex Mechanical Services; Central Sprinkler LLC; Chemguard, Inc.; Connect 24 Wireless Communications Inc.; Exacq Technologies, Inc.; FM Systems Europe Limited; FM Systems Group LLC; Grinnell LLC; Haz-Tank Fabricators, Inc.; Integrated Systems and Power, Inc.; IonicBlue Partners LLC; JC Residential and Light Commercial LLC; Johnson Controls (Suisse) SA; Johnson Controls Air Conditioning and Refrigeration, Inc.; Johnson Controls Building Automation Systems, LLC; Johnson Controls Building Solutions LLC; Johnson Controls Capital LLC; Johnson Controls Federal Systems, LLC; Johnson Controls Fire Protection LP; Johnson Controls Foundation, Inc.; Johnson Controls Government Systems, LLC; Johnson Controls, Inc.; Johnson Controls Navy Systems, LLC; Johnson Controls North America Products, LLC; Johnson Controls PI Project Site Operations LLC; Johnson Controls Security Solutions LLC; Johnson Controls-Hitachi Air Conditioning North America LLC; Johnson Controls US Holdings, LLC; M&M Refrigeration, LLC; Master Protection, LP dba FireMaster; Qoisy, Inc.; Rescue Air Systems; Retail Expert, Inc.; Richmond Alarm Company LLC; Security Enhancement Systems LLC; Sensormatic Electronics, LLC; Sensormatic USA LLC; ShopperTrak International Investment LLC; ShopperTrak RCT Corporation; Shurjoint America, Inc.; Silent-Aire USA Inc.; Silent-Aire Mission Critical Service LLC; Tyco Fire & Security LLC; Tyco Fire Products LP; Visonic Inc.; WillFire HC, LLC; York International (SA), Inc.; York International Corporation

# IL 10 (12/06) OLD REPUBLIC INSURANCE COMPANY

## ADDITIONAL INSURED - OWNERS, LESSEES OR CONTRACTORS - SCHEDULED PERSON OR ORGANIZATION - ENDORSEMENT A2

Named Insured Johnson Controls US Holdings, Inc.			Endorsement Number
Policy Prefix	Policy Number MWZY 313947 24	Policy Period 10/01/24 - 10/01/25	Effective Date of Endorsement 10/01/24
Issued By Old Republic Insurance Company			

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

### COMMERCIAL GENERAL LIABILITY COVERAGE PART

### SCHEDULE

#### Name Of Additional Insured Person(s) Or Organization(s):

If required by contract, the person or organization listed on the certificate of insurance as additional insured, and each other person or organization required to be included as an additional insured pursuant to a contract with a named insured.

#### Location(s) Of Covered Operations:

As required by contract.

Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

**A. Section II - Who Is An Insured** is amended to include as an additional insured the person(s) or organization(s) shown in the Schedule, but only with respect to liability for "bodily injury", "property damage" or "personal and advertising injury" caused solely by:

1. Your acts or omissions; or
2. The acts or omissions of those acting on your behalf;

In the performance of your ongoing operations for the additional insured(s) at the location(s) designated above.

**B. With respect to the insurance afforded to these additional insureds, the following additional exclusions apply:**

This insurance does not apply to "bodily injury" or "property damage" occurring after:

1. All work, including materials, parts or equipment furnished in connection with such work, on the project (other than service, maintenance or repairs) to be performed by or on behalf of the additional insured(s) at the location of the covered operations has been completed; or
2. That portion of "your work" out of which the injury or damage arises has been put to its intended use by any person or organization other than another contractor or subcontractor engaged in performing operations for a principal as a part of the same project.

GL 289 001 1012



# IL 10 (12/06) OLD REPUBLIC INSURANCE COMPANY

## ADDITIONAL INSURED - OWNERS, LESSEES OR CONTRACTORS - COMPLETED OPERATIONS - ENDORSEMENT A2A

Named Insured Johnson Controls US Holdings, Inc.			Endorsement Number
Policy Prefix	Policy Number MWZY 313947 24	Policy Period 10/01/24 - 10/01/25	Effective Date of Endorsement 10/01/24
Issued By Old Republic Insurance Company			

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

This endorsement modifies insurance provided under the following:

### COMMERCIAL GENERAL LIABILITY COVERAGE PART

#### SCHEDULE

##### Name Of Additional Insured Person(s) Or Organization(s):

If required by contract, the person or organization listed on the certificate of insurance as additional insured, and each other person or organization required to be included as an additional insured pursuant to a contract with a named insured.

##### Location And Description Of Completed Operations:

As required by contract.

Information required to complete this Schedule, if not shown above, will be shown in the Declarations.

**Section II - Who Is An Insured** is amended to include as an additional insured the person(s) or organization(s) shown in the Schedule, but only with respect to liability for "bodily injury" or "property damage" caused solely by "your work" at the location designated and described in the Schedule of this endorsement performed for that additional insured and included in the "products-completed operations hazard".

GL 289 002 1012



# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

4/28/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an **ADDITIONAL INSURED**, the policy(ies) must have **ADDITIONAL INSURED** provisions or be endorsed. If **SUBROGATION** IS **WAIVED**, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

<b>PRODUCER</b> Scott Insurance - Lynchburg 1301 Old Graves Mill Road Lynchburg VA 24502	<b>CONTACT NAME:</b> Lindsey Dejarnette <b>PHONE (A/C. No. Ext):</b> 434-832-2100 <b>FAX (A/C. No):</b> 434-832-2296 <b>E-MAIL ADDRESS:</b>
<b>INSURED</b> Driven Security, LLC 10645 N Tatum Blvd Ste 200-410 Phoenix AZ 85028	<b>INSURER(S) AFFORDING COVERAGE</b> <b>INSURER A :</b> Underwriters at Lloyd's London <b>INSURER B :</b> Acuity, A Mutual Insurance Company (A+) <b>INSURER C :</b> Accident Fund Insurance Company of America (A) <b>INSURER D :</b> <b>INSURER E :</b> <b>INSURER F :</b>

**COVERAGES****CERTIFICATE NUMBER:** 647692443**REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> <b>COMMERCIAL GENERAL LIABILITY</b> <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			SARPG-000008-01	2/1/2025	2/1/2026	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 100,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000 \$
B	<input checked="" type="checkbox"/> <b>AUTOMOBILE LIABILITY</b> <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY			ZY9691	3/1/2025	3/1/2026	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input type="checkbox"/> <b>UMBRELLA LIAB</b> <input checked="" type="checkbox"/> OCCUR <input checked="" type="checkbox"/> <b>EXCESS LIAB</b> <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			SARPGUMN-00008-01	2/1/2025	2/1/2026	EACH OCCURRENCE \$ 5,000,000 AGGREGATE \$ 5,000,000 \$
C	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y / N <input type="checkbox"/>	N / A	AF WCP 100124621	3/1/2025	3/1/2026	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
A	Professional Liability			SARPG-000008-01	2/1/2025	2/1/2026	Limit of Liability 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

**CERTIFICATE HOLDER****CANCELLATION**Polk County FL  
330 W Church Street  
Bartow FL 33830

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.



March 27, 2025

**POLK COUNTY, A POLITICAL SUBDIVISION OF THE STATE OF FLORIDA**  
**ADDENDUM #1**

**RFP 25-191, Polk County South & Central County Jail Security Upgrades**

---

This addendum is issued to clarify, add to, revise and/or delete items of the RFP Documents for this work. This Addendum is a part of the RFP Documents and acknowledgment of its receipt should be noted on the Addendum.

---

Contained within this addendum: Question and answer.

*Tabatha Shirah*

Tabatha Shirah

Procurement Analyst

Procurement Division

---

**This Addendum sheet should be signed and returned with your submittal. This is the only acknowledgment required.**

---

Signature: 

Printed Name: Adam Birdwell

Title: Owner

Company: Driven Security

**RFP 25-191, Polk County South & Central County Jail Security Upgrades**

**Addendum #1**

---

**Question 1:** 1) Can you confirm that RFP #25-191 Polk County South & Central County Jail Security Upgrades will not include Door Hardware such as locks and will be Security Controls Only? 2) If so, do you know if a separate RFP will be forthcoming for this work?

**Answer 1:** 1) This RFP will not include door hardware such as locks.  
2) The County has a separate solicitation that will be forthcoming replacing the Slider Cell Doors at the Central County Jail Only but it is not part of this RFP.

April 17, 2025

**POLK COUNTY, A POLITICAL SUBDIVISION OF THE STATE OF FLORIDA**  
**ADDENDUM #2**

**RFP 25-191, Polk County South & Central County Jail Security Upgrades**

---

This addendum is issued to clarify, add to, revise and/or delete items of the RFP Documents for this work. This Addendum is a part of the RFP Documents and acknowledgment of its receipt should be noted on the Addendum.

---

Contained within this addendum: Proposal receiving date extension, Questions and answers.

**The Proposal Receiving Date has been extended one (1) week. The revised Proposal Receiving Date is Wednesday, April 30, 2025, prior to 2:00 p.m.**

*Tabatha Shirah*

Tabatha Shirah

Procurement Analyst

Procurement Division

---

**This Addendum sheet should be signed and returned with your submittal. This is the only acknowledgment required.**

---

Signature: 

Printed Name: Adam Birdwell

Title: Owner

Company: Driven Security

**Question 1:** 1) Can you confirm that RFP #25-191 Polk County South & Central County Jail Security Upgrades will not include Door Hardware such as locks and will be Security Controls Only? 2) If so, do you know if a separate RFP will be forthcoming for this work?

**Answer 1:** 1) This RFP will not include door hardware such as locks. 2) The County has a separate solicitation that will be forthcoming replacing the Slider Cell Doors at the Central County Jail Only but it is not part of this RFP.

**Question 2:** Page 7, **Qualifications**, item #3 requires a completed SOC2 Type 2 report be submitted, and states that the SOC2 form is provided on the FTP site. The only document available on the FTP site is the "Polk County BoCC IT Vendor-Security-Questionnaire V4" Excel spreadsheet.

- 1) Is this Excel spreadsheet the SOC2 form?
- 2) If not, please provide the SOC2 form.
- 3) Under which Tab (Tabs 1-5) should this Excel spreadsheet be included in the electronic upload?

**Answer 2:** 1) Yes. 2) N/A. 3) Please place this items in "Tab 1, Executive Summary," after introduction letter.

**Question 3:** The subject RFP includes the following documents to be completed and returned with our proposal; under which Tab (Tabs 1-5) should these be included?

- a. Proposers Incorporation Information (Submittal Page) – RFP page 27
- b. Drug-Free Workplace Form – RFP page 28
- c. Affidavit Certification Immigration Laws – RFP page 32
- d. Employment Eligibility Verification (e-Verify) Certification – RFP page 33

**Answer 3:** Please place these items in "Tab 1, Executive Summary," after introduction letter.

**Question 4:** Page 8, **System Minimum Requirements, Door Controls**, includes the statement, "Electric strikes must meet appropriate ANSI/BHMAA A156.3 standards." Does the Agency anticipate the replacement of existing door locks and/or electric strikes? If so, please specify number and type.

**Answer 4:** This was for reference only. No door locks are anticipated during this project.

Addendum #2

---

**Question 5:** Does the Agency have a preferred low voltage/electrical contractor for the provision of conduit/cable where new cable may be needed (example: new CAT6 cable for new IP cameras)? If so, please provide the name and contact information for same.

**Answer 5:** Polk County doesn't have a preferred low voltage/electrical contractor.

**Question 6:** Regarding low bandwidth requirements, please designate which location(s) or area(s) would require additional bandwidth?

**Answer 6:** This would be required for the Cloud Base solution for incoming data transfers.

**Question 7:** Please designate which systems must be 'cloud based'.

**Answer 7:** The County would like the option for the camera system to be either cloud based or on premises.

**Question 8:** 1) Is not meeting the 10-year EIN requirement a strict disqualification or just a basis for consideration in the review process?

2) If a company has been in business under the same EIN for 8 years, but their owners and team have 10+ years of experience individually, would that meet qualification?

3) Request the County reduce qualification from 10 years in business under the same EIN to 5 years?

**Answer 8:** 1) It would disqualify your company.

2) No, the qualification is for the company not the individuals experience at your company.

3) The requirements in the Qualifications will not be reduced.

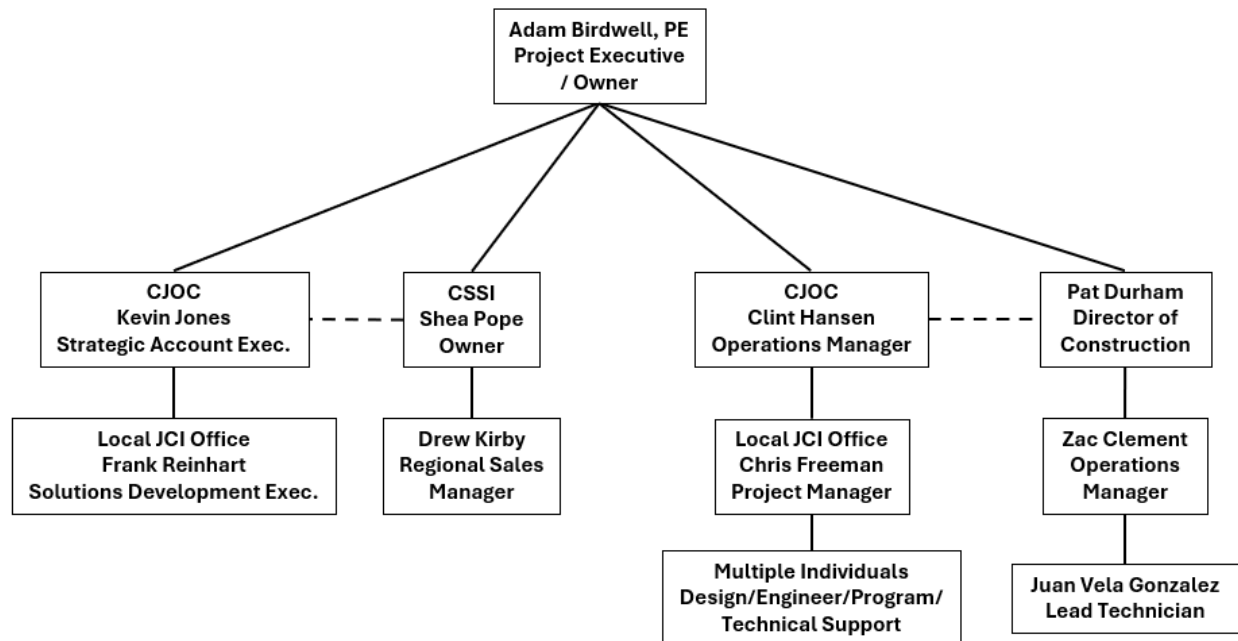
**Question 9:** Due to the required amount of Survey Questionnaires to be submitted with our RFP response, and the Easter/Spring Break holiday coming up, we respectfully ask for a two-week extension?

**Answer 9:** One-week extension approved, see page one of Addendum 2 for extension information.

## TAB 2

### Experience, Expertise, Personnel, & Technical Resources

#### Project Organization Structure



**SALES /  
PRECONSTRUCTION**

**OPERATIONS**

## Adam Birdwell, PE – Owner

241 Wilson Pike Circle  
Brentwood, TN 37027  
615.533.4503

Adam has over 20 years of experience in the industry leading teams in over \$400 million of work including Retail, Industrial/Manufacturing, Warehouses, Multi-family, Healthcare, Office, University, and Correctional projects. Adam is a licensed professional engineer in the state of Tennessee and is a LEED Accredited Professional. He also has his General Contractor's License, Low Voltage Electrical License, and Security / Alarm Systems License in multiple states.

### Employment History

#### **Driven Security**

Brentwood, TN  
2020 - Present

*Owner*

Oversee and manage all operations of the company

#### **The Graceway Group**

Brentwood, TN  
2020 - Present

*Owner*

Oversee and manage all operations of the company

#### **Elmington**

Nashville, TN  
2017 - 2019

*Vice President of Construction*

Oversaw all construction operations within the company. He was responsible for the supervision, direction, communication, and development of the Project Teams, ensuring the overall positive outcome of the projects. He aligned all aspects of the project to meet Internal and External Client Expectations. He ensured that successful client and subcontractor relationships were maintained. Adam's leadership allowed the project teams to deliver quality projects on time and under budget.

#### **Lithko Contracting**

Nashville, TN  
2013 - 2017

*Operations Manager*

Oversaw all operations of the BURG. Working closely with the project teams, he provided operational support to ensure a positive outcome for all projects. He engaged the team to develop an overall project plan and set expectations for the project. He validated project status and made recommendations to the project teams to

ensure that execution goals were met. Adam directed and aligned manpower resources to meet execution goals and ensure successful projects. Adam was responsible for maintaining customer relationships by staying engaged with the customers throughout the projects. Adam maintained communication with customer leadership to resolve any conflicts or issues that arose throughout the phases of projects.

## **Charter Construction**

Nashville, TN

2004-2013

### *Project Manager*

Adam used his engineering background to provide a high level of project management skill. His field work experience allowed him to communicate and work closely with field personnel as well as design professionals. He used the latest computer software and equipment to efficiently manage and provide timely information for the construction process. He was responsible for all aspects of the project from preconstruction to closeout. Once he created the schedules, he worked closely with field crews to manage the progress of the project. Adam prepared and approved shop drawings and submittals, using AutoCAD and other design and review software. Adam tracked job cost information and reviewed it with the teams in the field to ensure successful financial outcomes for the projects. He was also responsible for preparing monthly financials for review by company leadership and monthly billings to the owner/general contractor.

## **Certifications**

Licensed Professional Engineer

General Contractor

Licensed Security Technician

Licensed Qualifying Agent

LEED AP

Certified Verkada Engineer

Certified Verkada Sales Professional

Certified Verkada Access Control

Certified CEIA Technician

## **Project Experience**

Adams County Jail – Quincy, IL

Madison County Jail – Huntsville, AL

Buncombe County Jail – Asheville, NC

Mills County Jail – Goldthwaite, TX

Swain County Jail – Bryson City, NC

Lead Public Schools – Nashville, TN

Demopolis City Schools – Demopolis, AL

Westlake Academy – Westlake, TX

Virginia State University – Petersburg, VA

Summit BHC – Brentwood, TN

Marion County – Hamilton, AL



## **Kevin B. Jones – Strategic Account Manager**

**1281 Newell Parkway  
Montgomery, Alabama 36110  
334-309-1474**

### **Employment History**

#### **Simplex Time Recorder Co.**

Gardner Massachusetts

1992 - 1993

Electronic Estimator

Duties included but not limited to the following;

Specification reading and note irregularities

Device take off's

Preliminary design of integrated systems

#### **Simplex Time Recorder Co.**

Gardner, Massachusetts

1993 - 1994

Associate Sales Engineer

As an Associate Sales Engineer, my responsibility was to assist all Simplex districts in the design, lay out, and pricing for detention related integrated projects. Included traveling to train the local district's sales force on detention integrated projects and delivery.

#### **Simplex Time Recorder Co.**

Clearwater Florida

1994 - 1996

Assistant Project Manager/Engineer

During these two years I was responsible for the complete engineering and documentation for the Pinellas County Courthouse project, contract value \$1.4 million. Stationed "on-site", it was my primary duty to make sure all integrated systems were engineered, documented and installed correctly. I assisted with the installation, test check out, and training of the following systems; CCTV, Door Control, Intercommunications, Officer Duress System, Touch Screen Work Stations, Courtroom Video System, and Graphic Control Panels.

#### **SimplexGrinnell**

Prattville, Alabama

1996 - 2001

Senior Project Engineer

Serving as Senior Project Engineer – Responsibilities include complete design, engineering, testing, training and project close out documentation for at least 50 detention related projects that SimplexGrinnell districts secured.

## **SimplexGrinnell**

Prattville, Alabama

2001 - 2006

### **Detention Support Specialist**

As a Detention Support Specialist it was my duty to assist any and all SimplexGrinnell districts in the detention market. Duties included, training the local sales representative in the nuances of a detention project, obtain specifications and drawings and assist the local sales representative in bidding at least 75 integrated systems, presentations to Architects and Engineers to show case SimplexGrinnell's ability to design, deliver, close out a detention related project.

## **Johnson Controls – Legacy SimplexGrinnell**

Montgomery, Alabama

2006 - Present

### **Strategic Account Manager**

My duties are to track detention related projects, report the identified projects to the individual districts, coordinate and review project documents in conjunction with local District offices prior to the bidding of Criminal Justice Facilities to insure that Johnson Controls will comply with all of the requirements as indicated in the contract documents. Other duties include the complete design and pricing for integrated security systems, assign margin percentage dictated by current market.

## **Certifications – Include**

Fire Control Mechanic - Commonwealth of Massachusetts

Simplex - Basic building Systems Sales School

Folger Adams - Locking Systems

AirTeq - Locking Systems

Omron - PLC Systems

Allen Bradley - PLC Systems

American Dynamics -CCTV Systems

Burle - CCTV Systems

C-Cure – Access Controls

Megal Senstar – Perimeter Fence Systems / Microwave Systems

American Management Association – Fundamental Selling Techniques

American Management Association - Effective Presentation Skills

American Management Association - leadership Skills and Team Development

Federal Publications - CPM Scheduling in Mitigating & Analyzing Claims

Simplex - Fire Alarm Systems

## **Prior Association Member of**

American Jail Association

American Correctional Association

**Frank B. Reinhart**

4920 W. Melrose Ave. N.

Tampa, Florida 33629

[frank.reinhart@jci.com](mailto:frank.reinhart@jci.com)

Cell Phone: (813) 310-9770

**Summary of Qualifications and Achievements**

- Professional Account Executive with background of management positions
- Multiple Quota Club Achievers
- National Salesperson of the Year
- South East Region Salesperson of the Year

**Business Experience: 30 Plus Years Selling Business to Business**

***2015-Present: Johnson Controls Fire Protection***

Electronic Systems Account Executive: Marketing for Johnson Controls Fire Protection, which is a recognized leader in the manufacture, sales, and service of state-of-the-art monitor and control systems for Fire Alarm, Nurse Call, Video, Access Control, Integrated Systems, Portable Extinguishers, and Sprinklers Systems.

***2004-2015: Tyco Integrated Security/ADT***

Senior Account Executive: Marketing Integrated Security and Fire System Solutions Business to Business. Included products are Card Access, IP/Analog CCTV Systems, Fire Alarms and Burglar Alarms. Present Company, Conduct Surveys, Design Solutions, Present Proposals, Coordinate Installation and Training with customer in products usage and maintenance.

***1996-2004 The TeamWorks Personnel***

Vice President Sales: Established staffing service and generated sales from a first year level of \$270,000 to over \$2,800,000 in 2003. Sold Company

***1977-1996 Anacomp, Inc., Tampa, Florida.***

**Account Executive**

Sold Image and Information Management Solutions Business to Business. Included products were software, equipment, supplies, and services. Conducted surveys, presented seminars and trained clients in products usage and maintenance. Repeatedly exceeded quota and in top 10% nationally.

**Operations Manager**

Managed eighteen employees in a COM (Computer Output Microfiche ) service bureau. Responsible for programming, implementing and documenting all services output for 200+ customers. Consistently ranked in top 5% of Company standings for controlling cost, throughput and waste.

**Professional Affiliations:**

Data Processing Management Association (DPMA), President

**Education/Business Related Training:**

*Hillsborough Community College* Tampa, Florida, Graduate of *Plant High School*, Tampa, Florida. Multiple Sales Training Programs, Certificates received

## Shea Pope – Owner

241 Wilson Pike Circle  
Brentwood, TN 37027

615.772.7171

shea@drivenlocks.com

Shea is a hard working, driven, and focused strategic leader with over 20 years in executive management across multiple businesses. My daily passion is business development and through this desire I help organizations reach their goals. During my career to date I have assisted in helping three organizations reach over 10x revenue growth.

## Employment History

### **Driven Security**

Brentwood, TN

2014 - Present

*Founding Partner*

Oversee and manage all operations of the company

### **The Graceway Group**

Brentwood, TN

2020 - Present

*Owner*

Oversee and manage all operations of the company

### **Logo Brands**

Franklin, TN

2003 - 2020

*Partner*

Assisted in growing company revenue over \$28M as a partner. Sponsored multiple ERP conversions along with a WMS conversion. Assisted in obtaining rights to multiple professional sports leagues, and over 10 exclusive contracts with colleges across the country. Assisted in 2016 on an asset purchase to acquire new licensing rights. Helped facilitate management buyout in 2012. Assisted in growing company revenue over \$28M as a partner. Sponsored multiple ERP conversions along with a WMS conversion. Assisted in obtaining rights to multiple professional sports leagues, and over 10 exclusive contracts with colleges across the country. In my tenure led customer service, sales, shipping, IT, warehousing, procurement, quality assurance, etc... Integrator of software tying into SAP, MAS 200. In my tenure throughput increased from 500 orders to 7000 daily. Developed efficiency programs, training manuals, key performance metrics for employees. Created the "Ability to promise" inventory control that allowed for 50% less inventory. Revenue dramatically increased 50% from 2006-10, 60% from 2011-15, and 25% from 2016-18. I personally managed over \$2M of licensing contracts and over \$6M of E-commerce revenue operationally. Our team developed forecasting and analytic inventory ordering programs that lowered inventory to sales % to less than 8.5% yearly. Implemented automation directly with factories in China and Vietnam, saving 33% employee costs. Drove factory allocation

from four factories to twelve, and purchasing dollars increased from \$9M to \$16M yearly. Helped implement and oversee an office in China managing Quality assurance, factory orders and sourcing. Drove pricing down 10% across multiple factories. Developed deep experience in EDI, shipping, warehousing and distribution, IT, efficiency analysis of multiple departments, ERP management and selection, freight management and vendor relations.

#### *Regional Sales Manager*

Managed 450 sales accounts in a territory of accounts geographically all west of the Mississippi. Distribution channels ranged from mass accounts to startups. Responsible for over \$2 million dollars of revenue and I hit quota each year. During my time in this position company revenues grew 6x in 3 years. Managed 15 independent field reps across 12 states. I helped collaborate in product development as well. Also managed all things technical for the business including server management, ERP development and maintenance, and custom programming. Managed 450 sales accounts in a territory of accounts geographically all west of the Mississippi. Distribution channels ranged from mass accounts to startups. Responsible for over \$2 million dollars of revenue and I hit quota each year. During my time in this position company revenues grew 6x in 3 years. Managed 15 independent field reps across 12 states. I helped collaborate in product development as well.

#### **Mojetto LLC**

Collierville, TN

2009 - 2011

#### *Partner*

Helped increase revenues from \$60K to \$800K during my tenure in this sports licensed goods online E-commerce business. Brought specific knowledge of vendor and supply chain management. Increased vendor integrations from five companies to over forty at my exit. Implemented a state of the art customized order management platform that seamlessly integrated across Amazon, Amazon FBA, Sears E-comm, Ebay and others. Mojetto during my tenure was a top 10 E-commerce vendor for over 20 wholesale sports licensed customers.

#### **Education**

Liberty University

Bachelor of Business Administration, Accounting

#### **Certifications**

General Contractor

Licensed Security Technician

Licensed Qualifying Agent

Certified Security Systems Integrator

Certified Verkada Engineer

Certified Verkada Sales Professional

Certified CEIA Technician

#### **Project Experience**

Adams County Jail – Quincy, IL

Madison County Jail – Huntsville, AL

Buncombe County Jail – Asheville, NC

Mills County Jail – Goldthwaite, TX

Swain County Jail – Bryson City, NC

Lead Public Schools – Nashville, TN

Demopolis City Schools – Demopolis, AL

Westlake Academy – Westlake, TX

Virginia State University – Petersburg, VA

Summit BHC – Brentwood, TN

Marion County – Hamilton, AL

City of Oxford Jail – Oxford, AL

Ft. Payne City Schools AL

## Drew Kirby – Regional Sales Manager

241 Wilson Pike Circle  
Brentwood, TN 37027

321.749.7588

[drew@drivenlocks.com](mailto:drew@drivenlocks.com)

Drew has over 12 years of enterprise experience in the construction sales industry leading teams in the construction of over \$20 million of work including Retail, Industrial/Manufacturing, Warehouses, Healthcare, Office, and University projects. Drew is a licensed Verkada sales and technical engineer.

### Employment History

#### **Driven Security**

Brentwood, TN  
2023 - Present  
*Regional Sales Manager*

#### **Verkada**

Tampa, FL  
2022 - 2023  
*Account Executive*

#### **AmberBox Gunshot Detection**

Nashville, TN  
2021 - 2022  
*Sales Consultant*

#### **JumpCrew**

Nashville, TN  
2019 - 2021  
*Senior Account Executive*

#### **PLW Modelworks**

Melbourne, FL  
2013 - 2019  
*Geospatial Analyst*

### Certifications

Certified Verkada Engineer

Certified Verkada Sales Professional

### Project Experience

Madison County Jail – Huntsville, AL

Buncombe County Jail – Asheville, NC

Swain County Jail – Bryson City, NC

Demopolis City Schools – Demopolis, AL

Virginia State University – Petersburg, VA

## **Clint G. Hansen – Operations Manager**

---

**1281 Newell Parkway  
Montgomery, Alabama 36110  
334-309-1477**

### ***Employment History***

#### **Johnson Controls (Tyco-SimplexGrinnell)**

Operations Manager  
Criminal Justice Operations Center  
Montgomery, Alabama  
January 2007 to Present

Duties include: Supervision and management of operations with regard to the coordinated effort of the design and installation of integrated products in the correctional market. Develop custom interfaces and drivers for Integration of PLC Controllers to various 3<sup>rd</sup> party systems.

2001 – 2007, Senior Project Engineer  
1999 – 2001, Sr. Customer Support Rep / Project Engineer

#### **CDT Systems**

CEO/Owner  
Cedar Falls, Iowa  
1996-1999

Duties included: Supervision and management of the affairs of the corporation. Site assessments to determine appropriate solutions to meet customer requirements. Installation / service of Fire Alarm, Security, Telephone, and Nurse Call systems. Project management through construction/installation phases

#### **Reliable Systems**

Electronics Technician  
Waterloo, Iowa  
1994-1996

Duties Included: Installation / service of Fire Alarm, Security, Telephone, and Nurse Call systems.

### ***Education***

Hawkeye Community College – 1992-1994  
Waterloo, Iowa  
AAS in Electrical Engineering Technology

### ***Certifications – Include***

Wonderware InTouch Development  
InduSoft Web Studio Development  
Omron PLC Controllers & Software  
Allen-Bradley PLC-5 Controllers / RSLogix 5/500 Software  
Folger Adam Security Lock/Hardware Training  
StationX Cyber Security – Network Security Training

### ***Project Experience***

Central Nova Scotia Correctional Facility – Dartmouth, NS  
Circleville Juvenile Detention Facility – Circleville, OH  
Cleveland House of Corrections – Cleveland, OH  
Federal Correctional Institute – Phoenix, AZ  
Fort Leavenworth Regional Correctional Facility – Leavenworth, KS  
Greene County Jail – Springfield, MO  
Kaufman County Jail – Kaufman, TX  
Oklahoma County Jail – Oklahoma City, OK  
Ross Correctional Facility – Chillicothe, OH  
Sarasota County Jail – Sarasota, FL  
Buncombe County Jail – GE PLC – Asheville, NC



## **Christopher R. Freeman**

Sarasota, FL

(941) 730-0056

Christopher.Freeman@jci.com

### **Project Qualifications Summary**

Over 20 years of experience managing, installing, and servicing fire alarm and low-voltage systems across commercial, transportation, and healthcare sectors. Specializing in project coordination, permit acquisition, field installation management, and system commissioning. Successfully led complex fire alarm projects at Tampa International Airport and other high-profile facilities.

### **Certifications & Training**

- NICET III – Certification #139023
- OSHA 10-Hour Safety Training
- Factory Trained on:
  - Simplex: 4005, 4006, 4008, 4010, 4100+, 4100U, 4007ES, 4010ES, 4100ES
  - Zettler Sentinel 500 Nurse Call System

### **Relevant Project Experience**

#### **SimplexGrinnell LP / Johnson Controls Fire Protection**

Install Technician/Project Manager | October 2008 – Present

- Lead project manager for multi-phase fire alarm upgrades at Tampa International Airport.
- Coordinated directly with owner's representatives and general contractors to plan and execute installations.
- Scheduled manpower, managed material procurement, and maintained project timelines.
- Utilized Accela permitting portal and managed Notice of Commencement filings for Hillsborough County.
- Oversaw field technicians and installation quality control.
- Programmed and commissioned Simplex fire alarm and access control systems.
- Identified and executed change orders to accommodate project scope revisions.

#### **SimplexGrinnell LP**

Senior Fire Alarm Service Technician | September 2006 – October 2008

- Serviced and programmed fire alarm, access control, and nurse call systems.
- Specialized in diagnostics of circuit faults, grounding issues, and system malfunctions.
- Supported both warranty and long-term service contracts for commercial clients.

## Highlighted Project Contributions

- **\*\*Project 935362501 – West Jail Sally Port & Booking\*\*** (Feb 2009 – April 2010)

Served as the lead installer under Superintendent Bobby Belisle and Clint Hanson from CJOC. Responsible for wiring and final terminations of intercom devices, cameras, locks, PLCs, DVRs. System programming was completed by Clint w/CJOC.

- **\*\*Project 949545203 – SCJ Video Visitation\*\***

Acted as lead installer for the SCJ Video Visitation system under Superintendent Bobby Belisle. Completed all wiring and terminations of visitation system components. System programming was handled by Bobby Belisle and Herold Harrod.

- **\*\*Unnamed Visitation Project – Near Gainesville, FL\*\***

Acted as lead installer for the SCJ Video Visitation system under Superintendent Bobby Belisle. Completed all wiring and terminations of visitation system components. System programming was handled by Bobby Belisle

## Patrick Durham – Director of Construction

241 Wilson Pike Circle  
Brentwood, TN 37027  
270.339.4125  
pat@drivenlocks.com

Pat has over 25 years of experience in the industry leading teams in the construction of over \$600 million of work including Retail, Industrial/Manufacturing, Warehouses, Multi-family, Healthcare, Office, University, and Correctional projects.

### Employment History

#### **Driven Security / The Graceway Group**

Brentwood, TN  
2022 - Present

##### *Director of Construction*

Oversee and manage the development of the company's safety goals, processes and procedures. Support and mentored project teams companywide throughout the country. Coordination, schedule, budget, managed self-perform crews and managing subcontractors, inspections and the execution of the work.

#### **Elmington Construction**

Nashville, TN  
2018 - 2022

##### *Senior Superintendent*

Supported and mentored project teams for all of Elmington Constructions operations across the country on safety, coordination, schedule, budget, managing subcontractors, inspections and execution and performance of the work. I visited each site to support and mentor our teams.

#### **BL Harbert Int.**

Clarksville, TN  
2016 - 2017

##### *General Superintendent*

Coordinating schedule, budget, managed subcontractors, and inspection of all work performed. Met all contract and drawing requirements on time and under budget with high level security requirements.

#### **Taylor's Concrete**

Clarksville, TN  
2014 - 2016

##### *General Superintendent*

**QBS Inc**

Clarksville, TN

2011 - 2014

*General Superintendent*

Coordinating schedule, budget, managed subcontractors, processed and reviewed all submittals and inspection of all work performed. Construction of site, utilities, and. Met all contract and LEED requirements. Met all requirements of water and air intrusion plans.

**BL Harbert Int.**

Clarksville, TN

2006 - 2010

*General Superintendent*

Coordinating schedule, budget, managed subcontractors, processed and reviewed all submittals and inspection of all work performed. Construction of site, utilities, and. Met all contract and LEED requirements.

**Certifications**

General Contractor

Certified Verkada Engineer

Certified Verkada Sales Professional

Certified CEIA Technician

OSHA 30

CPR / First Aid

Rough Terrain Forklift

Aerial Work

Powder Actuated Tools

Fall Protection

**Project Experience**

Adams County Jail – Quincy, IL

Madison County Jail – Huntsville, AL

Buncombe County Jail – Asheville, NC

Mills County Jail – Goldthwaite, TX

Swain County Jail – Bryson City, NC

Lead Public Schools – Nashville, TN

Demopolis City Schools – Demopolis, AL

Westlake Academy – Westlake, TX

Virginia State University – Petersburg, VA

Summit BHC – Brentwood, TN

Marion County – Hamilton, AL

## Zac Clement – Operations Manager

241 Wilson Pike Circle  
Brentwood, TN 37027

731.333.4499

zac@drivenlocks.com

Honorably Discharged Special Operations Veteran with 19 total deployments with multiple agencies. Executive level experience running operations in multiple fields building and supervising teams and projects of all sizes globally. Successfully ran national marketing campaigns, organized major events, established multi-million-dollar partnerships, and oversaw international programs developing software and hardware. Built a specialized UAV program that was presented and eventually put into a program of record at the Pentagon.

## Employment History

### **Driven Security**

Brentwood, TN

July 2024- Present

*Operations Manager*

Oversee and manage team and project to ensure successful completion. Sourcing and ordering materials. Seek and develop new products and partnerships. Establish policies and procedures to maintain continued skill building, inventory management, personnel. Perform site walks to build complete plans for jobs to track and be as successful as possible.

### **goTenna**

New York, NY

October 2023-February 2024

*Program Manager/ Consultant*

Brought in to build policy and procedures for a technology start-up company with 100 plus million-dollar government contracts to build advanced software protocol and hardware to provide off grid mesh network communications. Wrote templates and trained project and program managers in tracking milestones and performance amongst multiple business units.

**MAG**

2017-2022

*Program Manager/ Director*

Provided site set up and operations for multiple sites in Africa, Afghanistan, Iraq, Lebanon and South America. Gathered operational intelligence for multiple agencies on high value targets. Created and executed plans for military and clandestine operations. Developed and maintained rotational deployment tracker for eighteen plus locations to ensure contract compliance, mission success capability and personnel request. Ensured staff maintained an elevated level of diligence and professionalism to provide mission performance for customer satisfaction. Approved and corrected timecards, expense authorizations, and expense reimbursement ensuring they were accurate and in compliance with company policies and contractual charge codes. Managed and oversaw day-to-day operations of flight, logistical, and sales teams in support of commercial UAS operations with full information briefings to team and government customer.

Built and maintained trackers for all personnel required documents and training. (Passport, VISA, network tokens, etc.). Over 5000 hours of PIC flight time on multiple platforms. Sourced contracts and companies to build secure living and operational compounds around the world. Built advanced surveillance infrastructure to include fiber networks, ground sensors, weather detection and electronic warfare systems.

**US Army Corp of Engineers**

Camp Arifjan, Kuwait

2013

*Electrical Project Manager/ NCOIC*

Ran all of the electrical projects for the 120 million dollar Gateway Project, turning Camp Arijan from a forward operating base to a permanent duty station. Building housing, restaurants, training facilities, athletic centers and office complexes. Oversaw and performed the design and installation of the entire electrical infrastructure. Converted all existing electrical to NEC compliance, transformed all international systems to US standards. Worked selecting contractors and ensuring compliance for contract completion. Submitted daily trackers and briefing for USDOD.

**Education**

University of TN Chattanooga  
Bachelor of Science-Sports Medicine  
Political Science Minor

**Certifications**

PMP Certification  
Licensed Security Technician  
NEC Residential Electrician  
Certified Security Systems Integrator  
Certified Verkada Engineer  
Certified Verkada Sales Professional  
Six Sigma Green Belt  
WPS trained and Certified  
Top Secret/SCI Security Clearance with Poly  
Certified CEIA Technician

## Juan Vela Gonzalez – Lead Technician

241 Wilson Pike Circle  
Brentwood, TN 37027

256.338.0346

[juan@drivenlocks.com](mailto:juan@drivenlocks.com)

Juan has over 20 years of experience in the industry leading teams in many project types including Retail, Industrial/Manufacturing, Warehouses, Healthcare, Office, University, and correctional projects.

### Employment History

#### **Driven Security**

Brentwood, TN  
2020 - Present  
*Lead Technician*

#### **Google Fiber**

Huntsville, AL  
2015 - 2020  
*Technician*

#### **Charter**

Huntsville, AL  
2010 - 2015  
*Technician*

#### **Spectrum**

Huntsville, AL  
2005 - 2010  
*Technician*

#### **Seismic Oil Fields**

2002 - 2005

### Certifications

Certified Verkada Engineer

Certified Verkada Sales Professional

Certified Verkada Access Control

Certified Alarm / Low Voltage Technician

### Project Experience

Adams County Jail – Quincy, IL

Madison County Jail – Huntsville, AL

Buncombe County Jail – Asheville, NC

Mills County Jail – Goldthwaite, TX

Swain County Jail – Bryson City, NC

Lead Public Schools – Nashville, TN

Demopolis City Schools – Demopolis, AL

Westlake Academy – Westlake, TX

Virginia State University – Petersburg, VA

Summit BHC – Brentwood, TN

Marion County – Hamilton, AL

City of Oxford Jail – Oxford, AL

Ft. Payne City Schools AL



## TAB 2

### Experience, Expertise, Personnel, & Technical Resources

#### Similar Project Experience

##### Johnson Controls – National Leader in Correctional Facility Systems Integration

Johnson Controls brings decades of proven success in the design, engineering, and integration of security control systems for county, state, and federal correctional institutions. With hundreds of successful installations nationwide, Johnson Controls is an established expert in deploying:

- **Harding Intercom Systems** – Specifically engineered for detention environments, Harding systems are a staple in correctional-grade communications. Johnson Controls is one of the most experienced system integrators of Harding intercoms, having implemented solutions across maximum-security prisons and county jails alike.
- **Omron PLC Control Systems** – Johnson Controls' technical team specializes in designing programmable logic controller (PLC) networks for automating cell doors, gates, sally ports, HVAC controls, and emergency overrides with robust system redundancy and lockdown capability.
- **Aveva InduSoft HMI Integration** – Their in-house engineers develop user-friendly graphical interfaces that provide operators with real-time visibility and control of facility-wide systems, ensuring intuitive operation and streamlined incident response.

This experience includes full life-cycle project delivery — from engineering and permitting, through installation, commissioning, and support — tailored specifically for secure, 24/7 operational environments.

---

##### Driven Security – Scalable Surveillance & Low Voltage Expertise in Critical Sectors

Driven Security has extensive experience in municipal, educational, and law enforcement environments, particularly in delivering Verkada-based camera upgrades and low-voltage infrastructure deployment across multi-building campuses and public facilities.

Key areas of expertise include:

- **Verkada Surveillance Upgrades** – Driven Security has deployed Verkada CD and CH series cameras in more than 200+ mission-critical sites, including city halls, police departments, school campuses, and





fire stations. Their team is proficient in strategic placement, edge recording, analytics configuration, and secure remote access provisioning.

- Low Voltage & Structured Cabling – All projects include comprehensive low voltage wiring, PoE camera networks, patch panels, rack design, and network switch integration — executed to ANSI/TIA standards and tailored for future scalability.
- Municipal Compliance & Law Enforcement Coordination – Their team is accustomed to working within the operational parameters and compliance requirements of government-owned facilities, including security clearances, shift-sensitive work schedules, and integration with public safety systems.

---

#### Combined Capabilities: Purpose-Built for Correctional Facility Upgrades

Together, Johnson Controls and Driven Security offer a complementary, full-scope solution that aligns precisely with the needs outlined in the RFP:

- Johnson Controls provides unmatched experience with intercom, PLC, and SCADA/HMI system upgrades in corrections.
- Driven Security delivers advanced, scalable video surveillance, cabling, and system deployment services grounded in municipal, law enforcement, and education sector projects.

Both firms bring the required technical depth, project capacity, and operational familiarity to ensure a secure, timely, and mission-focused upgrade of the county correctional facility's integrated security system.



## TAB 2

### Experience, Expertise, Personnel, & Technical Resources

#### Similar Project Experience

PROJECT Reference #1:Client name: JCI - Hamilton County, TN

**REMOVED BY PROCUREMENT**



## Project Reference #2 – Madison County AL Law Enforcement Countywide Upgrade

### Contact Person:

Lt. Scott Brown

Operations Manager – Madison County Sheriff's Office

### Contact Phone Number and Email Address:

Phone: (256) 555-2041

Email: sbrown@madisoncountyal.gov

### Cost of the Project:

\$1,600,000

### Start and End Date of Project:

Start Date: September 20, 2020

Completion Date: April 16th, 2025

### Brief Description of Services Provided and Why the Customer Needed the Solution:

Madison County sought to modernize outdated surveillance systems at its **main county jail, service center and county courthouse**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance and access platform**.

The project included:

- **Deployment of Verkada CD42 cameras** to cover interior corridors, holding cells, interrogation rooms, and administrative areas
- **CD52 cameras** for perimeter and parking coverage
- Centralized management through **Verkada Command software**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for law enforcement staff and IT administrators
- Post-deployment monitoring and support

This solution provided the County with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified evidence retrieval, and stronger facility access control.

### Number of Devices Installed:

- **400 cameras total:**
  - 350 Verkada CD-series (indoor)
  - 50 Verkada CD52 (outdoor)
- **40 viewing stations**



PROJECT Reference #3:Client name: JCI - Ohio Department of Rehab and Corrections

**REMOVED BY PROCUREMENT**



## Project Reference #4 – Adams County IL Law Enforcement Countywide Upgrade

### **Contact Person:**

David Hochgraber  
IT Director – Adams County Illinois

### **Contact Phone Number and Email Address:**

Phone: (217) 277-2161  
Email: dhochgraber@co.adams.il.us

### **Cost of the Project:**

\$910,000

### **Start and End Date of Project:**

Start Date: January 27, 2023  
Completion Date: 4/16/2025 (change orders and additional products added)

### **Brief Description of Services Provided and Why the Customer Needed the Solution:**

Adams County sought to modernize outdated surveillance and access control systems at its **police headquarters, municipal jail, and county courthouse, along with all other county buildings**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics. Most of the county buildings were using various different systems for security.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance and access platform**.

The project included:

- **Deployment of Verkada CD42, CD52, CH52 and CD62 cameras** to cover interior corridors, holding cells, interrogation rooms, and administrative areas
- **CH52 multisensor cameras** for perimeter and parking coverage
- **Verkada Access Control** units to secure all restricted doors and integrate badge-based staff access
- Centralized management through **Verkada Command software for all county buildings**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for law enforcement staff and IT administrators
- Post-deployment support
- Camera call up integration from the Control Room to Verkada

This solution provided the County with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified evidence retrieval, and stronger facility access control. The finance and IT teams can predict better how much the security systems will cost over the life of use.



A big factor in the purchase was the ability to see all cameras and access control in one platform. David told us that the 10 year warranty on Verkada products, along with the 24/7 US based support was a deciding factor. Our team has been by the customer's side during the first two years of use, performing training and guidance as issues arise.

**Number of Devices Installed:**

- **480 cameras total**
- **210 access control doors** connected to Verkada controllers
- **40 viewing stations**
- **10 intercoms**
- **24 environmental sensors**



PROJECT Reference #5:Client name: JCI – Buncombe County, NC

**REMOVED BY PROCUREMENT**



## Project Reference #6 – Marion County AL Schools Countywide Upgrade

### Contact Person:

Patrick Sutton  
Superintendent – Marion County Schools

### Contact Phone Number and Email Address:

Phone: (205) -412-6859  
Email: psutton@mcbe.net

### Cost of the Project:

\$1,600,000

### Start and End Date of Project:

Start Date: September 1st, 2024  
Completion Date: December 31<sup>st</sup>, 2024

### Brief Description of Services Provided and Why the Customer Needed the Solution:

Marion County Schools sought to modernize outdated surveillance systems at its **various educational facilities**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance platform**. The project included:

- **Deployment of Verkada CD62 cameras** to cover hallways, classrooms and recreational facilities
- **CH52 multisensor cameras** for perimeter and parking coverage
- Centralized management through **Verkada Command software**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for staff and IT administrators
- Post-deployment monitoring and support

This solution provided the County with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified evidence retrieval, and stronger facility control.

### Number of Devices Installed:

- **715 cameras total:**
  - 660 Verkada CD-series (indoor)
  - 55 Verkada CH52 (outdoor multisensor)

This facility is currently undergoing a second phase to add access control to all schools based on how well the Verkada cameras have performed, along with how well the sale and installation did as well.





PROJECT Reference #7Client name: JCI – Nova Scotia Correctional Facility, Canada

**REMOVED BY PROCUREMENT**



## Project Reference #8 – Lead Schools Systemwide Upgrade

### Contact Person:

Maggie Stampley

Admin – Lead Schools

### Contact Phone Number and Email Address:

Phone: (615) 800-8293

Email: [maggie.stampley@leadpublicschools.org](mailto:maggie.stampley@leadpublicschools.org)

### Cost of the Project:

\$700,000

### Start and End Date of Project:

Start Date: April 1, 2024

Completion Date: February 1, 2025

### Brief Description of Services Provided and Why the Customer Needed the Solution:

Lead Schools sought to modernize outdated surveillance and access control systems at its **main offices, classrooms and exterior of over five separate campuses**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance and access platform**.

The project included:

- **Deployment of Verkada CD42 and CD52 cameras** to cover **main offices, classrooms and exterior of over five separate campuses**
- **CH52 multisensor cameras** for perimeter and parking coverage
- **Verkada Access Control** units to secure all exterior doors and integrate badge-based staff access
- Centralized management through **Verkada Command software**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for staff and IT administrators
- Post-deployment monitoring and support

This solution provided the school system with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified video retrieval, and stronger facility access control.

### Number of Devices Installed:

- **200 cameras total:**
  - 140 Verkada CD-series (indoor)
  - 60 Verkada CH52 (outdoor multisensor)
- **40 access control doors** connected to Verkada controllers



## Project Reference #9 – Swain County NC Law Enforcement Countywide Upgrade

### Contact Person:

Jason Gardner  
Director – Swain County Jail

### Contact Phone Number and Email Address:

Phone: 828-488-0159  
Email: jbgardner@swaincountync.gov

### Cost of the Project:

\$261,000

### Start and End Date of Project:

Start Date: August 1, 2024  
Completion Date: October 1, 2024

### Brief Description of Services Provided and Why the Customer Needed the Solution:

Swain County sought to modernize outdated surveillance systems at its **municipal jail**, and **county courthouse**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance**. The project included:

- **Deployment of Verkada CD42 and CD52 cameras** to cover interior corridors, holding cells, interrogation rooms, and administrative areas
- **CH52 multisensor cameras** for perimeter and parking coverage
- **Integrated Verkada camera call ups for detention officer use**
- Centralized management through **Verkada Command software**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for law enforcement staff and IT administrators
- Post-deployment monitoring and support

This solution provided the County with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified evidence retrieval, and stronger facility access control.

### Number of Devices Installed:

- **100 cameras total:**
  - 75 Verkada CD-series (indoor)
  - 25 Verkada CH52 (outdoor multisensor)



## **Project Reference #10 – Buncombe County NC Law Enforcement Countywide Upgrade**

### **Contact Person:**

David Thompson

IT Director – Buncombe County Jail

### **Contact Phone Number and Email Address:**

Phone: (828) 775 - 6704

Email: David.Thompson@buncombenc.gov

### **Cost of the Project:**

\$612,000

### **Start and End Date of Project:**

Start Date: February 12, 2023

Completion Date: November 1, 2023

### **Brief Description of Services Provided and Why the Customer Needed the Solution:**

Buncombe County sought to modernize outdated surveillance systems at its **Jail headquarters, county courthouse, and county wide facilities**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance**. The project included:

- **Deployment of Verkada CD42, CH52 multisensors and CD52 cameras** to cover interior corridors, holding cells, interrogation rooms, and administrative areas
- **CH52 multisensor cameras** for perimeter and parking coverage
- **Integrated camera callups for detention officers to view**
- Centralized management through **Verkada Command software**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for law enforcement staff and IT administrators
- Post-deployment monitoring and support

This solution provided the County with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified evidence retrieval, and stronger security control.

### **Number of Devices Installed:**

- **300 cameras total:**
  - 240 Verkada CD-series (indoor)
  - 40 Verkada CD52
  - 20 Verkada CH52 (outdoor multisensor)
  - 8 Viewing Stations



## **Project Reference #11 – Auburn Housing Authority AL Systemwide Upgrade**

### **Contact Person:**

Richetta Stephens

Admin – Auburn Housing Authority

### **Contact Phone Number and Email Address:**

Phone: (480) 555-2041

Email: [samantha.reyes@fairmontcity.gov](mailto:samantha.reyes@fairmontcity.gov)

### **Cost of the Project:**

\$400,000

### **Start and End Date of Project:**

Start Date: September 1, 2020

Completion Date: April 1, 2025

### **Brief Description of Services Provided and Why the Customer Needed the Solution:**

Auburn Housing sought to modernize outdated surveillance systems at its **government housing projects across the county**. The legacy infrastructure lacked remote access, reliable storage, and intelligent video analytics.

**Driven Security** was selected to provide a turnkey upgrade using **Verkada's cloud-native surveillance and access platform**.

The project included:

- **Deployment of Verkada CD42 and CD52 cameras** to cover all interior and exterior areas of the housing projects
- **CD52 cameras** for perimeter and parking coverage
- Centralized management through **Verkada Command software**
- Full **Cat6A structured cabling**, switch configuration, and PoE deployment
- Training for staff and IT administrators
- Post-deployment monitoring and support

This solution provided the County with secure, scalable, and remotely manageable infrastructure, enabling real-time visibility, simplified video retrieval, and stronger security control.

### **Number of Devices Installed:**

- **150 cameras total:**
  - 120 Verkada CD-series (indoor)
  - 30 Verkada CD52 (outdoor)



## TAB 3

### Approach to Project

Driven Security and Johnson Controls have established a highly effective partnership grounded in mutual expertise, seamless coordination, and a shared commitment to delivering high-quality, integrated security solutions for critical facilities. Together, our teams have successfully executed multiple facility security upgrades, combining Johnson Controls' industry-leading experience in PLC automation, intercom systems, and HMI interfaces with Driven Security's expertise in advanced surveillance, access control, and low-voltage infrastructure.

Throughout the design and build phases of past projects, our companies collaborated closely — aligning engineering disciplines, streamlining timelines, and maintaining open communication with clients and stakeholders to ensure minimal disruption to facility operations. We leveraged our complementary strengths to deliver turnkey systems that were fully tested, thoroughly documented, and tailored to each facility's operational demands.

As we look at Polk County in particular, both Driven Security and Johnson Controls remain fully committed to continuing this partnership in the service of your County. Together, we offer the capacity, experience, and long-term dedication required to support the county's security modernization goals across both large correctional facilities ensuring safety, scalability, and operational resilience for years to come.

Below is a general outline of our approach to the work of these projects:

#### **1) Operator Control Room Workstations**

- a) Due to the different technologies at each facility, (Central with "Analogue Switch / LED" & South with "IP Computers") the concept will be that all existing Control Rooms will receive:
  - i) Computer
  - ii) 27" Touch Monitor
  - iii) GUI Software License
  - iv) UPS for an approx. 15 – 20-minute runtime
- b) Existing "monitor and control" apparatuses as explained above (analogue / IP), will be removed and new equipment will be installed.
- c) If any existing Control Room at either facility needs new consoles, the existing will be removed and replaced with new modern ergonomical consoles.
- d) Each facility will be provided with one (1) spare PC that can be used in any location.

## 2) Programmable Logic Controllers

- a) Due to the different technologies at each facility, (Central with “No PLC - considered hardwired” & South with “PLC - considered current technology”) the concept will be that all existing Equipment Rooms will receive:
  - i) **Central** – Complete Rip & Replace of all existing control equipment and be replaced with up-to-date PLC and downstream equipment (relays / fuses / power supplies etc.)
  - ii) **South** – Complete Rip & Replace of existing PLC equipment only and be replaced with up-to-date PLC and all downstream equipment will remain.
    - (1) Due to the standard downstream equipment which is considered up-to-date even though it was installed years ago, it is not necessary to remove, this will save costs on equipment, labor and most importantly downtime when converting over to the new system.
      - (a) However, in future interviews, if the county would like this equipment to be replaced, then when it comes to the pricing, this will be included.
- b) Existing field device wiring will remain and be re-terminated on new system.
- c) Existing field devices will remain.
- d) Will re-utilize existing head-end enclosures.
- e) All new equipment will receive a UPS for an approx. 15 – 20-minute runtime.

## 3) Intercom and Page

- a) Due to the different technologies at each facility, (Central with “Building Stand-Alone” & South with “Networked IP”) the concept will be that all existing Control Rooms / Equipment Rooms will receive:
  - i) Control Rooms – VoIP Master Station
    - Type of Master Station to be discussed at future interviews / meetings
  - ii) Equipment Rooms – Digital Controllers
    - Quantity of controllers to be decided by quantity of existing stations wired to each room.
- b) Existing field device wiring will remain and be re-terminated on new system.
- c) **NOTE: without proper inspections of existing field intercom stations, it is anticipated that all existing intercom stations will be replaced**
- d) Existing page speakers will remain.
  - i) Current page zones will stay the same.
- e) New Page Amplifiers will be provided.
- f) The new system will be equipped with Audio Threshold Detection, which is a software-based selection.
- g) Audio Recording Server will be provided.
- h) Will provide new head-end enclosures at all locations where appropriate or utilize existing rack space where appropriate.

**4) Camera System**

- a) The overall layout of the new cameras will be designed to meet or exceed the existing coverage, addressing any potential existing blind spots.
- b) We will utilize all of the types of cameras that are available to us to provide the best possible design for Polk County
- c) We will utilize viewing stations in control rooms and other strategic locations to maximize the effectiveness of the new integrated system.
- d) 24/7 US based support, 10 year warranty on hardware
- e) Storage can be recorded or live view only as desired
- f) Storage can be chosen up to 365 days as desired
- g) Secure camera housing that is vandal proof
- h) Unlimited user capacity and capability
- i) RTSP streams from the cameras will be utilized for integration with the touch screen camera call ups
- j) Compliant hardware and software that is up to code on all UL and NDAA requirements

**5) Security Management System (Reports)**

- a) A new SMS with a printer will be provided for each facility so that all security commands made within the detention facility will be logged
- b) The SMS will be installed in the Central Control room

**6) Networking Equipment / Infrastructure**

- a) POE + switches shall be provided and configured per the specifications of the county
- b) We recommend a complete new network infrastructure at the central facility
- c) South's network infrastructure could potentially be re-used but we recommend new network switches at a minimum

**Additional Services / Labor:**

- 1) Operator Workstation Screen/Icon review meetings
- 2) Un-Termination of existing field device wiring
- 3) Removal of existing equipment stated above
  - a) Will be handed over to owner for their discretion to keep or throw away
- 4) Installation of new equipment stated above
- 5) Re-termination of existing field device wiring to new equipment
- 6) Detailed enclosure drawings (head-end equipment)
- 7) Head-end point-to-point drawings
- 8) Programming for new systems
- 9) Head-End equipment fabrication (where applicable)
- 10) Complete systems PRE and POST test of existing field devices
- 11) Pre-Commission of upgraded areas (when completed independently) and a full commission once all areas have been upgraded (see proposed schedule)
- 12) Owner Training





- a) Operator Training will be 4 - 4-hour sessions
  - b) Maintenance Training will be 2 - 4-hour sessions
- 13) Final Documentation (as-builds)

**Additional Comments / Conditions:**

- 1) Diagnostics or repair for any existing field device and / or wiring
  - a. If an existing field device is found inoperable while completing the Pre-Test of existing systems, this device will be noted.
  - b. If the failed device is still inoperable after the Post-Test, a quote will be provided for time and material to repair
- 2) A secure gateway module will be provided so that technicians can tunnel into system and check health, provide diagnostics and / or programming changes
- 3) No integration of existing Fire Alarm / Building Automation Systems has been discussed at this time
- 4) Initially the equipment will be warranted for one (1) year unless additional years are appropriate (10) per the RFP through the negotiations



Based up the limited amount of specific information provided about each facility, it is difficult to provide a hard schedule, but based upon previous project experience, we would expect the work at each facility to take 12-24 months. Below is a rough outline of the expected project phases:

Project Schedule: PLC, Camera, and Intercom Upgrade at Correctional Facility

Timeline	Phase	Key Activities
TBD	Project Kickoff	<ul style="list-style-type: none"><li>- Stakeholder meeting</li><li>- Site access planning</li><li>- Security clearance processing</li></ul>
TBD	Site Assessment	<ul style="list-style-type: none"><li>- Evaluate existing systems</li><li>- Inventory hardware</li><li>- Identify integration points</li></ul>
TBD	Design & Engineering	<ul style="list-style-type: none"><li>- Finalize upgrade specs (PLC, IP cameras, intercoms)</li><li>- Develop system architecture &amp; wiring diagrams</li></ul>
TBD	Procurement	<ul style="list-style-type: none"><li>- Order equipment (cameras, PLCs, intercoms, switches)</li><li>- Confirm delivery timelines</li></ul>
TBD	Infrastructure Preparation	<ul style="list-style-type: none"><li>- Run conduit and cabling</li><li>- Prep equipment racks and electrical panels</li></ul>
TBD	Equipment Delivery & Staging	<ul style="list-style-type: none"><li>- Receive and inspect hardware</li><li>- Configure and pre-program systems offsite</li></ul>
TBD	Installation	<ul style="list-style-type: none"><li>- Install PLCs in control rooms</li><li>- Mount cameras and intercom units</li><li>- Terminate wiring</li></ul>
TBD	Integration & Programming	<ul style="list-style-type: none"><li>- Integrate camera feeds with VMS</li><li>- Configure PLC logic</li><li>- Sync intercom endpoints</li></ul>
TBD	Testing & Commissioning	<ul style="list-style-type: none"><li>- Conduct full system test</li><li>- Verify failover and security protocols</li></ul>
TBD	Training	<ul style="list-style-type: none"><li>- Train correctional staff and maintenance personnel on system use and basic troubleshooting</li></ul>
TBD	Project Closeout & Handover	<ul style="list-style-type: none"><li>- Final walkthrough and punch list</li><li>- Deliver documentation (as-builts, manuals)</li><li>- Obtain client sign-off</li></ul>



## QA / QC

Our teams have established a comprehensive Quality Assurance (QA) and Quality Control (QC) program to ensure the delivery of high-quality products and services across their operations. The programs integrate robust supplier management, continuous improvement methodologies, and advanced digital tools to uphold and enhance quality standards.

### Johnson Controls

#### **1. Global Supplier Performance Standards Manual (GSPSM):**

This manual outlines Johnson Controls' expectations for suppliers, emphasizing compliance with international standards such as ISO 9001:2015 for quality management, ISO 14001:2015 for environmental management, and ISO 45001:2018 for occupational health and safety. Suppliers are required to demonstrate their commitment to integrity, ethics, and quality through appropriate management standards.

#### **2. Six Sigma Methodology:**

Johnson Controls employs Six Sigma methodologies to achieve high-quality outcomes. Suppliers are expected to adhere to these practices, aiming for less than 250 defective parts per million (DPPM) for direct materials and a 15% reduction in supplier-related warranty events.

#### **3. Issue Resolution Information System (IRIS):**

To address and resolve quality issues efficiently, Johnson Controls utilizes IRIS, a system designed for tracking and managing supplier-related quality concerns. This tool facilitates communication and corrective actions between Johnson Controls and its suppliers.

#### **4. Continuous Improvement Initiatives:**

The company integrates Lean Manufacturing and Six Sigma programs with critical thinking methodologies to drive continuous improvement. This approach focuses on eliminating waste, reducing variation, and solving complex problems to enhance operational efficiency.

#### **5. Digital Tools and Training:**

Johnson Controls offers training services through its Training Institute, providing courses on HVAC, Building Automation Systems (BAS), and Variable Refrigerant Flow (VRF) systems. These programs ensure that technicians are well-equipped to maintain and improve quality standards.

## Driven Security

### 1. Service Design & Implementation

- **Integration with Industry Standards:** We ensure that all security solutions comply with relevant industry standards and regulations, providing clients with reliable and compliant systems. We do this by selecting manufacturers that comply with all local, state and federal compliance.

### 2. Personnel Training & Certification

- **Comprehensive Training Programs:** Implement ongoing training for all staff members to stay updated on the latest Verkada security technologies and protocols.
- **Certification Requirements:** Encourage and support staff in obtaining relevant Verkada certifications to maintain a high level of expertise within the team.

### 3. System Monitoring & Maintenance

- **Regular System Audits:** Conduct periodic audits of security systems to ensure optimal performance and identify areas for improvement.
- **Preventive Maintenance:** Establish a schedule for routine maintenance to prevent system failures and ensure continuous protection for clients.

### 4. Client Feedback & Continuous Improvement

- **Feedback Mechanisms:** Implement channels for clients to provide feedback on services, facilitating ongoing improvements and client satisfaction.
- **Performance Metrics:** Track key performance indicators to assess the effectiveness of security solutions and make data-driven enhancements.

### 5. Emergency Response & Incident Management

- **Incident Response Plans:** Develop and maintain comprehensive incident response strategies to address potential security breaches or system failures promptly.
- **Post-Incident Analysis:** After any security incident, perform thorough analyses to understand root causes and implement measures to prevent future occurrences.



## TAB 4

### Software, Equipment, and Devices

For the camera needs in your facilities, our team is proposing the use of Verkada cameras. Verkada is one of the leading physical security providers in the world. Their solutions stand out for their ease of deployment and user-friendly design, ensuring that any team, regardless of technical expertise, can implement them in environments ranging from local offices to a global network of distributed sites. The following brochures outline their entire offering of products. We have also included specific data sheets of their top cameras in each of their product lines. They provide a wide range of options that can meet any need including pan-tilt-zoom (PTZ), multi-sensor, fisheye, bullet (with license plate recognition), and dome cameras.

These cameras are easily accessible through Verkada Command as well as Verkada's Viewing Stations and also seamlessly integrate into the overall integrated security system that we are proposing below. All camera streams will be able to be called up by the touch screen interface that controls all integrated solutions working in conjunction with the new digital intercom and locking control system. The viewing stations allow you to view up to 36 cameras simultaneously on a monitor from a simple plug and play network device. Verkada cameras offer up to 365 days of onboard and/or cloud storage. An unlimited amount of users may access your account at no additional cost. Verkada has built-in audit logs, tamper detection, and role-based controls that meet strict government compliance and security policies. Verkada provides 24/7 USA based remote support with an industry leading 10 year Verkada hardware warranty. Their product lines include everything from environmental sensors to guest management systems. Cellular gateways are also available to meet the needs of any remote locations without current network access. Verkada cameras can provide for the current needs of your facilities as well as needs that may arise in the future.

The products discussed below will complete the integrated security system for your facility. They are industry standard and non-proprietary. We will hand over all programming files and as-built drawings after the commissioning of your system. This provides you with full control of your system and the ability to manage it in the future as you see fit. Data sheets have been provided for all of the primary components of the system. We will utilize Dell workstations for the operator control rooms, Omron PLCs, Harding intercoms, and Dell servers for your security management system (SMS reports).

Harding intercoms are engineered for detention applications with ruggedized, tamper-resistant stations. They support selecting communication to pods, gates, control rooms, and administrative offices. They allow full automation of door releases, alarm triggers, and lockdown procedures through Omron PLC control.



Omron PLCs will control all physical access points (cell doors, mantraps, sallyports, etc) and can control environmental systems (lighting, ventilation, etc) with high reliability. They are expandable and scalable with modular architecture that accommodates future system growth and programming updates. Their fast I/O and system response is vital for rapid sequencing and safe zone-based control in emergencies.

A complete integrated security system for your facility provides many strategic benefits. Surveillance, control, and communication systems on a unified, responsive platform combine to provide end to end visibility. Automating core operations while empowering staff with real time intelligence and rapid response tools enhances safety and control. Reducing manual monitoring demands, maintenance overhead, and communication lags creates operations efficiency. We look forward to the opportunity to provide a live demo of our technologies to your team proving the capabilities of our system and that we are the best choice to partner with your county.



# Leading Cloud Physical Security for the Modern Law Enforcement Agency

Power smart policing with  
next-gen security technology  
and AI-driven analytics.

# Leading Cloud-Based Physical Security

Legacy security systems may no longer be equipped to handle today's evolving threats. Law enforcement agencies need real-time, actionable intelligence and flexible solutions to solve crimes more efficiently, especially with fewer resources. Join top police and sheriff departments who are setting a new standard in physical security and investigations with Verkada's cloud-managed platform. Empower your department with better intelligence to proactively protect your community.





# Why Law Enforcement Agencies Choose Verkada

Experience a new level of simplicity with Verkada. All you need is the hardware and access to Command, our software platform, which updates automatically. Centrally manage all Verkada devices and users from any browser or mobile device. Gain actionable insights with information integrated across devices.

**Access footage from anywhere** and rapidly investigate with AI-powered search

**Empower officers and staff** with a user-friendly and intuitive interface

**Enable monitoring anywhere** with easy-to-deploy mobile monitoring units

**Out-of-the-box integration with Axon Fusus** for more efficient investigations

**IT-friendly** with bandwidth-efficient cameras and no DVRs/NVRs to upkeep

**Easy access management** with granular user permissions

**Up to 10-year warranty**, predictable renewal costs, and unlimited user seats

**Top-rated technical support** – available 24/7 via email, phone, or live chat

**High-level security and compliance** – SOC 2 Type 2, ISO 27001/27017/27018, and FY2019 NDAA, TAA, and FIPS-validated camera models.

**Built on Zero Trust principles** with Enterprise Controlled Encryption (ECE), SSO, MFA, and SAML authentication

## Lancaster Police Department

"Our all-in-one platform allows us to efficiently oversee health, safety, and security, enhancing community protection. This technology not only supports rapid law enforcement response but also serves as a deterrent."

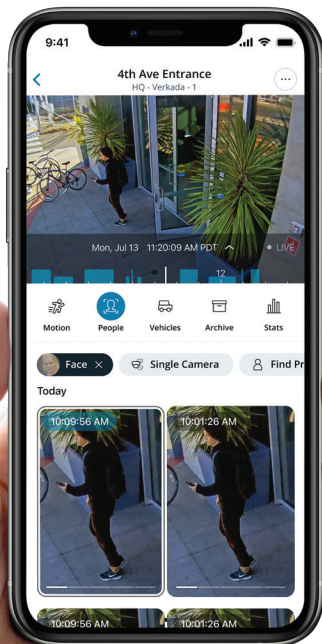
**Rodrick Armalin,**  
Chief of Police



## Hopewell Police Department

"During our initial deployment year, we observed a 38% reduction in major crime rates in the community."

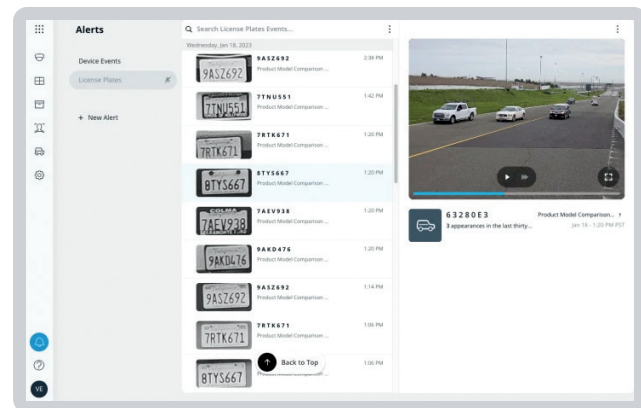
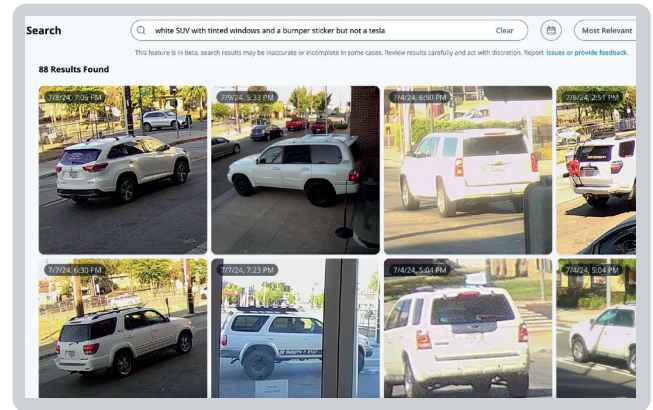
**Donnie Reid,**  
Deputy Chief



# Level Up Your Real-Time Crime Center and Rapidly Solve Crimes with AI

## Gather actionable intelligence in real time

- Leverage Verkada's License Plate Recognition (LPR) technology and AI analytics to quickly track suspect vehicles by entering a description (such as make and color) or a license plate.
- Pair LPR bullet cameras with multisensors or PTZs at intersections to capture not just a photo, but vital video context that reveals the vehicle's details and movements.
- Locate suspects or missing persons by uploading a photo or filtering by people's attributes. See where they've been spotted across your entire camera fleet, including non-Verkada cameras when connected via Command Connector.



## Leverage live alerts for smart policing

- Get immediate alerts on mobile or desktop whenever Verkada cameras detect a vehicle or license plate of interest (LPOI) that matches your criteria.
- Easily add plates or upload a bulk CSV file to automatically track vehicles linked to serious crimes.
- Set up persons of interest (POI) alerts to receive instant notifications whenever suspects or missing persons appear across any of your cameras.

## Unify cameras with Fusus integration

- Verkada's out-of-the-box integration with the Axon Fusus open platform enables law enforcement agencies to conduct more efficient investigations from a single view.
- Access and manage Verkada video data, including detected license plates, directly from FususONE to enhance situational awareness and response coordination.

## Streamline evidence management

- Leverage Verkada's built-in incident management tool to simplify case tracking. Quickly consolidate video evidence from multiple cameras into a single, shareable repository, giving investigators better context and clarity on each incident.
- Plus, with direct integration to Axon Evidence, easily save footage from Verkada cameras into Axon for streamlined digital evidence storage and management.

# Enhance Public Safety with Powerful Agile Solutions



## Resolve traffic disputes with objective data

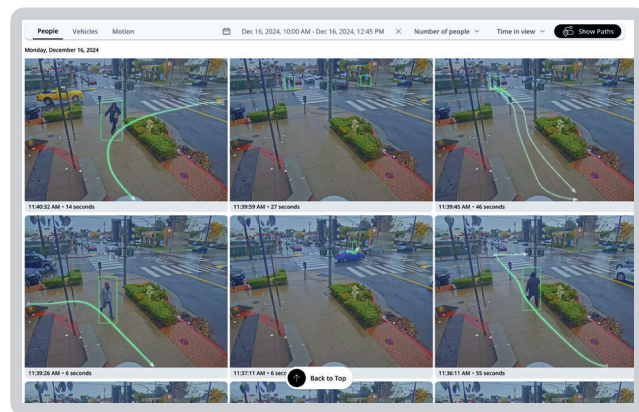
- Dispatch teams can share real-time intel or a direct footage link with officers on scene, reducing reliance on potentially biased witness accounts.
- Using trajectory analysis, dispatchers and officers can quickly assess the movement paths of people and vehicles to determine fault in traffic accidents.

## Accelerate response to school emergencies

- Verkada enables schools to quickly grant law enforcement access to an entire floor plan and its cameras via direct links or user accounts, helping dispatchers provide real-time intel to enhance officer safety and guide crisis response.
- Additionally, when law enforcement agencies use the same platform as schools, officers can save critical time by navigating a system they already know.

## Monitor anywhere with mobile video solutions

- Easily set up streetlight and mobile monitoring units with Verkada cameras, cellular gateways, and solar power solutions via trusted partners. PoE simplifies installation by powering cameras using a single cable, enabling quick setup.
- Effortlessly monitor outdoor events and help local businesses combat theft and vandalism. Conveniently share live camera feeds via text or a link to keep businesses informed and responsive.



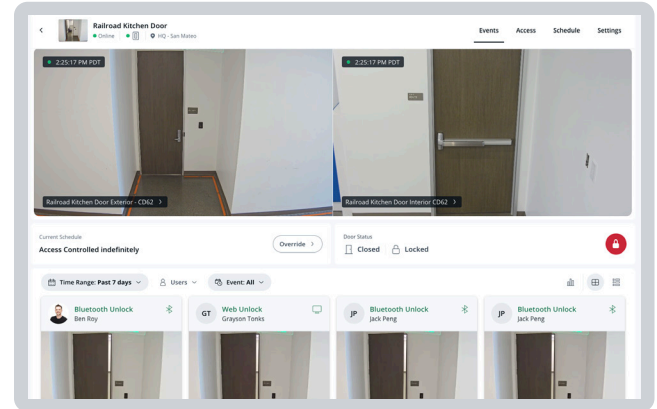
## Expand patrol coverage with virtual monitoring

- With limited personnel, maintaining 24/7 patrol coverage over city- and county-operated buildings can be a challenge. Maximize resources by using Verkada cameras as AI-powered alarms that alert for motion, people, or vehicles after hours.
- Trained monitoring agents are available to video verify alarms before notifying your teams and dispatchers.

# Optimize Station Operations for Greater Efficiency and Security

## Control critical access points

- Restrict access to sensitive areas like interview and records rooms with cloud-based access control. Easily set role-based permissions, automate door schedules, and configure time-based access for community events.
- Officers can use mobile credentials to enter secured areas, reducing reliance on physical keys or keycards that can be easily misplaced.
- With integrated video security, view not only written but also visual logs of door events to support faster investigations.



## Optimize sally port security

- Fisheye cameras provide a panoramic 180-degree view of the sally port, reducing blind spots to provide fuller visibility during prisoner transport. Footage can be easily downloaded or shared via a direct link for use in court.
- Operators can easily verify arriving police vehicles and remotely unlock sally port doors with integrated video security and access control, maximizing security during detainee handling.

## Streamline station workflows

- Simplify lobby operations with video intercoms that let officers see visitors at the door or assist remotely when the front desk is unattended.
- Speed up visitor check-ins with Verkada Guest by digitally capturing photo IDs and forms, while automatically notifying the assigned detective when a visitor arrives.
- In holding cells, video intercoms allow officers to communicate with detainees remotely, minimizing in-person interactions and enhancing officer safety.

## Protect critical evidence and IT equipment

- Air quality sensors in evidence and server rooms, paired with integrated access control and video security, help safeguard critical assets while providing audit trails of who accessed these areas.
- Receive instant SMS alerts for changes in conditions like temperature or humidity, helping to preserve evidence integrity and ensure the uptime of essential IT systems.

# One Platform to Simplify Law Enforcement Security

## Video Security

AI-enabled cameras provide 24/7 recording, up to 365 days of onboard storage, and industry-leading image quality. No DVRs or NVRs needed - just a PoE connection.

## Intercom

Protect and monitor entrances, lobbies, and holding cells - answer calls from anywhere with sharp video, clear audio, and four smart receiver methods.

## Guest

Simplify visitor check-ins by digitally capturing photo IDs and forms, while automatically notifying the assigned detective when a visitor arrives.

## Access Control

Manage station doors and employee credentials at scale with easy-to-deploy controllers and cloud-managed access control software.

## Air Quality Sensors

Protect critical evidence and IT equipment with instant alerts for temperature, humidity, noise, TVOCs, and other air quality indicators.

## Alarms

Detect intrusions and reduce false alarms with a cloud-based alarm system that provides full visibility into every alarm and features built-in professional monitoring.

## Connectivity

Easily deploy Verkada cameras with gateways that deliver power and data for mobile monitoring or in hard-to-wire locations like streetlights and parking lots.

## Mailroom

Streamline delivery management by tracking package drop-offs with a simple mobile scan and automatically notifying recipients upon delivery.

## Viewing Station

Stream up to 300 live camera feeds from multiple locations into a single command center, providing real-time visibility across the city or county.

## Try Verkada for free

Our 30-day free trial includes a device, two-way shipping, and full access to the Command management platform. Learn how we can support your smooth transition to the cloud by bridging non-Verkada devices to our cloud-based system.







Trusted by Leading Law Enforcement Agencies



East Greenwich  
Township Police  
Department



Winston-Salem  
Police Department



Parkersburg Police  
Department



Lancaster Police  
Department



Hartford Police  
Department



Hopewell Police  
Department



Arlington Police  
Department



Havre de Grace Police  
Department



## The Power of the Verkada Platform for Government Organizations

Verkada's government-grade offerings are designed to help government organizations and their partners take a proactive, simple, and scalable approach to physical security, alongside numerous security enhancements that are critical for certain government users.

### FedRAMP Ready at the Moderate Impact Level

Our solutions have undertaken rigorous security assessments like FedRAMP (FedRAMP Ready at the Moderate impact level), FIPS 140-2 validation, and TAA and FY 2019 NDAA compliance across three product lines.

### Security and Compliance\*

#### Zero Trust



## Government-grade physical security solutions

### Command in AWS GovCloud

Government customers in the United States can choose to use Verkada Command hosted in AWS GovCloud, which gives them the flexibility to use our secure cloud solutions on top of the additional stringent security controls provided by AWS GovCloud. Command in AWS GovCloud supports our FIPS-validated camera models and Verkada Guest.

### FIPS-Validated Cameras

Verkada's [FIPS-validated cameras](#) incorporate encryption that meets the FIPS 140-2 and FedRAMP Ready (Moderate) standards. They have durable, vandal-resistant designs, advanced computer vision features, and are TAA and FY 2019 NDAA compliant.

### Verkada Guest

Verkada Guest is a visitor management solution that allows government organizations to streamline check-in and provide a more welcoming experience for their visitors. Native camera integration helps organizations increase security by enabling them to immediately find footage of visitors as they move throughout the facilities.

### Why Verkada



#### Proactive security

Increase security and visibility with real-time alerts, the ability to share live links with authorities, and more.



#### Manage site from anywhere

Verkada lets you easily manage sites remotely from our intuitive Command mobile app – no port-forwarding or VPNs.



#### Protect privacy

Maintain security while protecting privacy with granular permissions, face blurring, privacy regions, and more.



#### Receive dedicated support

Our team can provide one-on-one support for system design, pricing, installation, integration, onboarding, and training

### Learn more

To learn more about Verkada for government-grade deployments, visit our site or email [government@verkada.com](mailto:government@verkada.com).

\*Not applicable to all products and models. Contact sales to inquire about the security and compliance features of individual product models.



# Leading in Cloud Physical Security

Protect people and places in a  
privacy-sensitive way.



# Table of Contents

About Verkada	4-5
Verkada Command	6-7
Video Security	8-11
Command Connector	12-13
Connectivity	14-15
Access Control	16-19
Video Intercom	20-23
Alarms	24-29
Air Quality Sensors	30-33
Workplace	34-39
Try Verkada for Free	40-41



# Built for Modern Enterprises

At Verkada, our mission goes beyond reinventing physical security; we empower organizations with AI-enabled devices and an enterprise-ready cloud platform to transform their approach to safety with infrastructure flexible enough to adapt quickly to changing security *and* business needs.

Organizations of all sizes, from local businesses to leading global brands with thousands of sites, use Verkada to improve their physical security practices — and have unlocked new operational efficiencies and savings in the process.

Our solutions stand out for their ease of deployment and user-friendly design, ensuring that any team, regardless of technical expertise, can implement them in environments ranging from local offices to a global network of distributed sites.

It's this scalability, combined with our advanced AI capabilities, that enables our customers to make more informed decisions every day.







# One Platform to Manage Security Across All Your Sites

Verkada Command is a cloud-based platform that integrates insights across the entire suite of Verkada products, including video security, access control, video intercom, air quality sensors, alarms, visitor management, and mailroom management.

## **Manage from anywhere**

Access all your Verkada devices and manage physical security on the go from our intuitive Command app.

## **Scale with ease**

Add an unlimited number of devices, sites, and users to Command's centralized platform without complicating the user experience.

## **Live event-based monitoring**

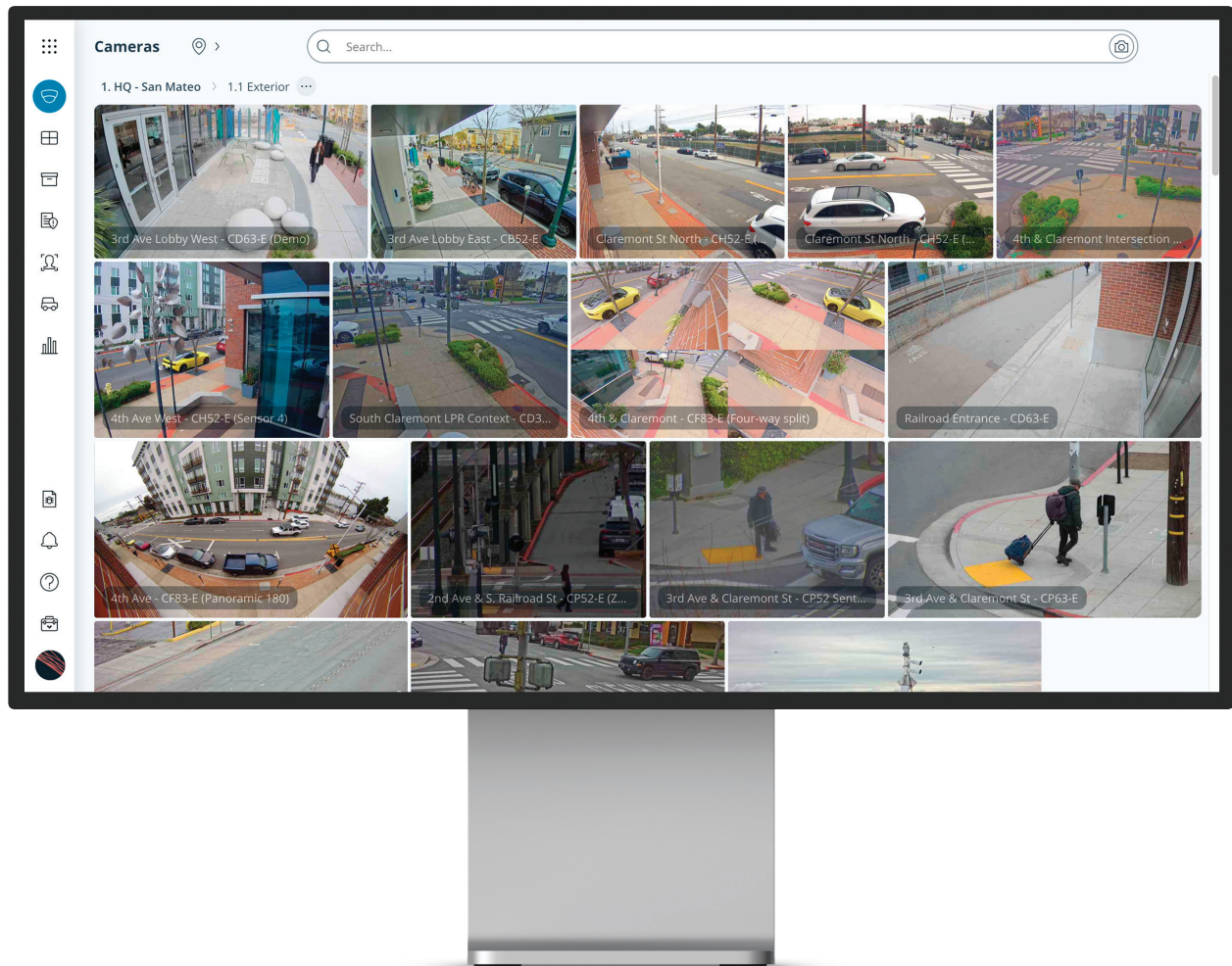
Gain real-time visibility into all devices across all sites from a single pane of glass.

## **Seamless user management**

Help ensure platform security with role-based access, single sign-on, two-factor authentication, and integrations for SCIM and SAML.

## **Zero-touch maintenance**

Automatic updates continuously deliver the latest features and security enhancements.



## Explore Command

Scan the QR code or visit [verkada.com/command](https://verkada.com/command) to discover why Command is not just another video management platform.





# Powerful Video Security with Hybrid Cloud Storage

High-resolution video security cameras offer the reliability of on-device storage with the flexibility of cloud archiving, providing teams with the most scalable way to store critical footage.

## **Reduce hardware overhead**

No NVRs, DVRs, or on-prem servers to manage. Cameras feature built-in onboard storage with up to 365 days of retention.

## **No single point of failure**

Even in the event of network outages, cameras record locally; once connectivity is restored, feeds are available for viewing.

## **Bandwidth-friendly**

Rather than streaming footage around the clock, cameras only stream when viewed and operate at just 20-50 kbps in steady state.

## **Quickly surface meaningful events**

Verkada cameras utilize the latest in AI and edge-based processing to uncover actionable insights in real time.

## What is Hybrid Cloud Video Security?



### Cameras

- Up to 365 days of onboard storage; No NVRs or DVRs
- Bandwidth-friendly (20-50 kbps in steady state)
- Single Ethernet cable (PoE) to operate

### Cloud (AWS)

- Seamless access to all cameras
- Unlimited archiving
- Enterprise Controlled Encryption (ECE)
- 30-days cloud backup included; can be extended further

### Software

- Intuitive browser-based user interface
- Modern user authentication (SSO, 2FA, SAML)
- No plugins or downloads required

“With DVRs and NVRs, you have to guess how much storage is left while maintaining at least a 30-day history. Depending on how many cameras there are or any issues that arise, you might discover only 14 days of video footage are available when there should be 30 to 90 days. With a hybrid cloud infrastructure, reliability is no longer a concern; video data is saved both onboard the camera and to cloud-based servers.”

Marshall Frost,  
IT Director, VP of Corporate Systems, Avita Pharmacy



# A Wide Range of Options to Meet Any Need

## Watch Demo

See how Verkada provides  
the most scalable, actionable,  
and easy-to-use video security  
solution on the market.





### **Dome Series**

Durable and versatile, the Dome Series features up to 4K sensor resolution and powerful onboard processing for an enhanced streaming experience.



### **Bullet Series**

Built to withstand harsh environments, the Bullet Series captures crisp details at a distance and powers a highly performant and accurate license plate recognition (LPR) experience.



### **Mini Series**

Designed for flexibility without compromise, the Mini Series features low-profile form factors that deliver exceptional image quality.



### **Fisheye Series**

Best for dynamic viewing, the Fisheye camera captures footage in a 180° panoramic view, a four-way split view, or an immersive view with digital pan-tilt-zoom.



### **Multisensor Series**

Ideal for expansive coverage and efficient installation, the Multisensor camera packs four independent camera systems into a single device.



### **PTZ Series**

Take control with 360-degree pan, 220-degree tilt, up to 32x optical zoom, and enjoy the ultimate live monitoring experience.

# The On-Ramp to Verkada's Cloud-Based Command Platform

Command Connector enables organizations to connect third-party, non-Verkada cameras to Command, allowing them to access powerful video analytics and capabilities using their existing infrastructure.

## **Enable a frictionless cloud migration**

Access the cloud in minutes and plan your organization's cloud transition while keeping within budget.

## **Experience an intuitive, single pane-of-glass management platform**

Connect as many non-Verkada cameras as you need to Command's simple and powerful UI and manage all your cameras from one screen. Use non-Verkada cameras as context cameras to enhance your Verkada Access Control, Air Quality Sensors, and Guest deployments.

## **Accelerate investigations with analytics**

Bridge your legacy cameras to Command and unlock advanced video analytics for your organization — enabling you to reduce investigation times from hours to minutes.





# Connect Any Verkada Device, Anywhere

The GC31-E and GW31-E gateways make it simple to deploy Verkada products anywhere with cell signal or Wi-Fi, including hard-to-wire locations such as parking lots, equipment yards, or streetlight poles.

## **Deploy anywhere**

Deploy Verkada anywhere with purpose-built LTE and Wi-Fi gateways. Feed the gateway any power source, connect to a cell carrier or Wi-Fi network, and send both power and data to any Verkada device via PoE.

## **Plug-and-play setup**

With the ability to tap into nearly any power source and send 60W across 2 PoE outputs, Verkada gateways are the easy button for deploying physical security anywhere.

## **Cloud-managed**

Easily set up and manage gateways in Verkada Command from any device and any location. See all your gateways on a map, remotely run diagnostics, and receive alerts if connectivity is lost.





# Smarter Access Control, Managed in the Cloud

Verkada Access Control combines easy-to-install hardware with intuitive cloud-managed software to provide you with a solution to secure every site, door, and user.

## **Every site**

Verkada's cloud-based system configures instantly with easy-to-install hardware that seamlessly connects to the Verkada Command software platform.

## **Every door**

Connect wired, wireless, online, or offline doors to Verkada Command to configure and connect every door in your organization.

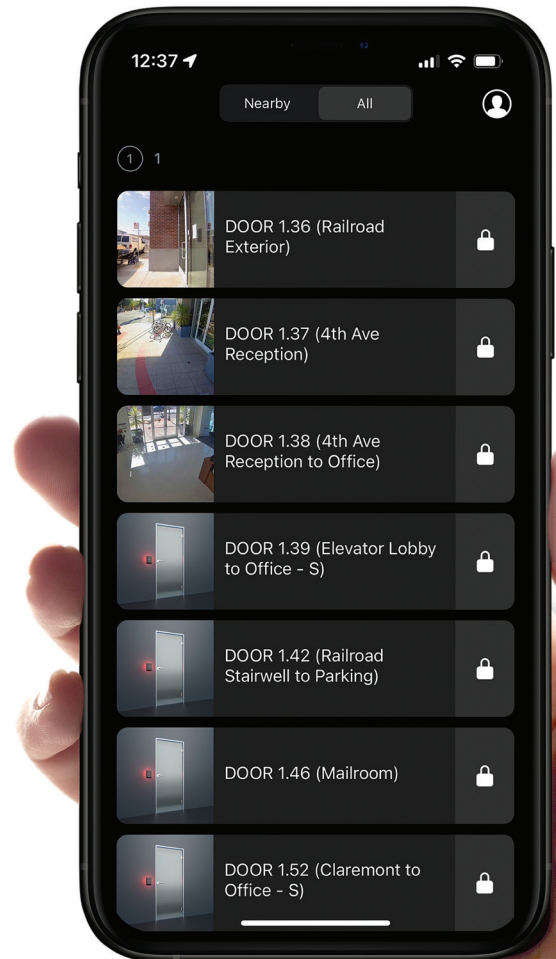
## **Every user**

Integrate user profiles from your single sign-on system and configure user profiles in Command to easily design, print, and issue physical or mobile credentials.

# Unlock Doors with the Verkada Pass Mobile App

Use any smartphone as a hands-free digital keycard to increase organizational security by eliminating lost badges, streamline credential provisioning with single sign-on (SSO) integrations, and give end users more flexibility with a convenient, mobile-based access method.

- Enable Bluetooth Low Energy (BLE) unlock for touchless entry.
- Activate lockdowns in real time.
- Easily assign, restrict, and revoke access to users.





# Simple to Install, Always Up-to-Date

## **One-door controller**

The AC12 one-door controller brings cloud-managed access control to standalone doors that would otherwise be difficult to secure with an electronic system.

## **4-door and 16-door controllers**

Designed for large organizations, the AC42 (a 4-door controller) and the AC62 (a 16-door controller) install easily and integrate seamlessly with existing door readers, AUX relays, and fire alarm interface panels.

## **Multi-format door readers**

The AD34 and AD64 door readers deliver simultaneous support for low and high frequency card formats to provide a secure and intuitive entry experience for secure, high-traffic doors.

## **IO controller**

With 16 AUX inputs and 16 outputs, the AX11 IO Controller integrates more of your building infrastructure into the Verkada ecosystem — including elevators, sensors, switches, and peripherals.

## **Wireless locks**

Manage more doors with Verkada's wireless lock integrations — compatible with select wireless locks from Schlage, Assa Abloy, and SimonsVoss.



**“** If we have another emergency situation, we need to be able to lock our campus down instantly. Verkada had everything I was looking for in an access system: centralized control, cloud-based, no servers required, and intuitive enough that I don’t need to spend a day training people how to use it. **”**

Alex Wiltz,  
Director of Public Safety, Chief of Police, and Emergency Management Coordinator  
Greenfield Community College

# Effortless Calling and Security at Scale

Answer calls, easily manage entry, and ensure your organization is secure with Verkada's cloud-managed video intercom.

## **Simplified entry**

The TD33, TD53, and TD63 intercoms are equipped with a reader, allowing authorized individuals to enter using a variety of credentials. The TD63 also features a keypad, making it easy to grant pincode access and implement multi-factor authentication at any entryway.

## **Unparalleled call quality**

Leverage sharp video across diverse lighting conditions and clear audio in any environment to easily communicate with anyone at the door.

## **Flexible receiver options**

Take calls from the lobby using Desk Station, or with additional receiver types on mobile, web browser, and existing telephone systems.

## **Management at scale**

Verkada's cloud-based management platform, Command, brings visibility and control at scale for many intercom systems across multiple sites.





# Take Calls from Anywhere

Bring flexibility to intercom calling with multiple receivers and cloud-managed call routing functionality.

## **Verkada Desk Station**

An iPad-based interface for receptionists, guards, and other stationed professionals to monitor live feeds and respond to calls with one-tap controls.

## **Verkada Pass App**

A mobile app for designated users to receive call alerts and respond on the go with one-tap controls, even if they are away from an entryway or computer.

## **Verkada Command**

A web browser-based interface for designated users to receive call alerts and field single or concurrent calls with one-tap controls.

## **Existing phone numbers**

An integrated way for organizations to receive intercom calls via their phone systems — like PSTN, SIP/VoIP, or Microsoft Teams — and respond with their dial pad.





# A Modern, Software-First Alarm System

Detect, verify, and respond to intruders across hundreds of sites with a single alarm solution that you can manage from anywhere. 24/7 professional monitoring comes included with Verkada Alarms.

## **Use sensors, cameras, or both**

Detect intruders with sensors, cameras, or both. Pair cameras with sensors for video verification, or use Verkada cameras themselves as AI-powered alarm triggers.

## **Reduce costly false alarms**

Screen out false alarms with camera triggers for person detection, loitering, and line-crossing. Reduce false dispatches by enabling video verification without costly integrations.

## **Stay calm and informed during an alarm**

Alarm notifications include a clear summary, relevant footage, and a live incident report, helping users confidently decide whether to cancel the alarm or dispatch police.

## **Easy to manage and IT-friendly**

Instead of calling the alarm company and incurring service fees, admins can manage every aspect of their alarm system via Verkada Command, even when not on site.





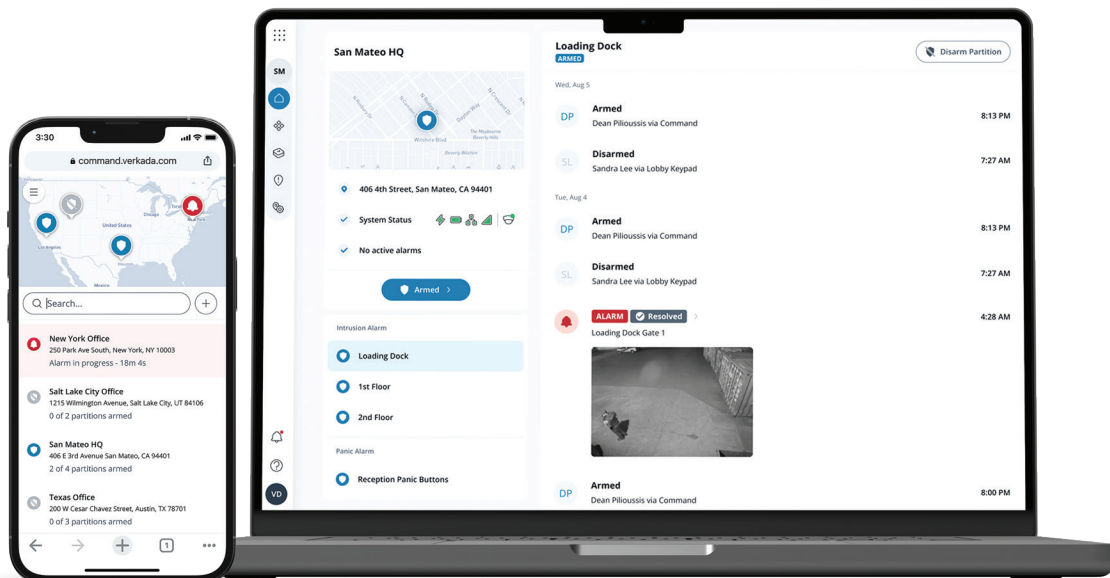
# An Alarm System That Puts You in Control

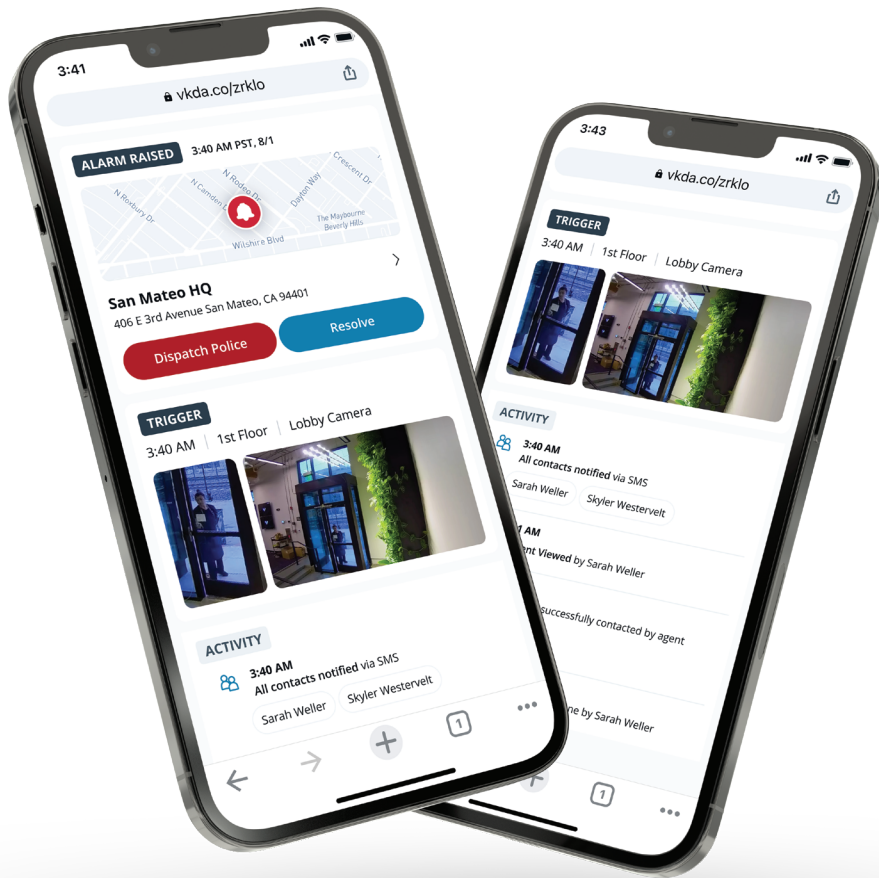
Verkada Alarms puts organizations in full control of their alarm sites via intuitive, cloud-based software.

Get remote visibility into alarm events and manage every aspect of the system from anywhere, eliminating the need to send staff on site or call the alarm company.

## Oversee all sites remotely

Review alarm events and manage every aspect of your alarm sites from anywhere, eliminating the need to call the alarm company and incur costly service fees.





## See the full picture of every alarm

Know exactly what triggered the alarm, who was contacted, and what actions the agent took. Users can view associated camera footage and agent call transcripts in the same place.

# AI-Based Video Alarms

In addition to traditional sensors, organizations can use Verkada cameras to trigger alarms. With AI person detection, Verkada cameras can screen out false alarms and extend protection outdoors.

## Reduce false alarms with AI

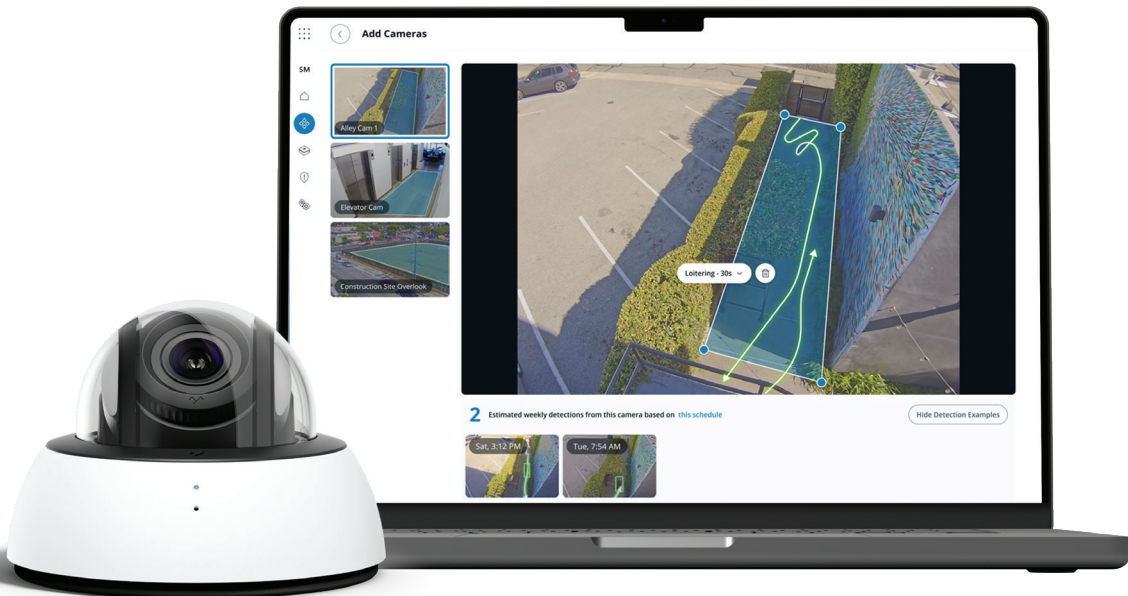
Set intelligent triggers like person detection, line-crossing, and loitering to screen out non-human activity and passerby traffic.

## Always human-verified

When a camera is triggered, monitoring agents will video-verify the event before raising an alarm.

## Extend protection outdoors

With camera triggers, organizations can easily protect outdoor areas such as fenced equipment yards and access-controlled loading docks.



# 24/7 Professional Monitoring



Verkada Alarms comes with 24/7 professional monitoring, which provides a team of trained agents who can respond to alarms.

## False alarm reduction

Agents can video-verify and dismiss false alarms, preventing late night phone calls and false police dispatches.

## Quick deterrence

Agents can talk down intruders through a powerful horn speaker to deter them from doing damage.

## Informed dispatch

Before dispatching police, agents can call designated contacts who can easily pull up video footage to make an informed decision.

# Better Air Quality Monitoring With Verkada

Ensure safe environments and optimize building performance with Verkada's all-in-one air quality sensors.

## **Instant SMS alerts**

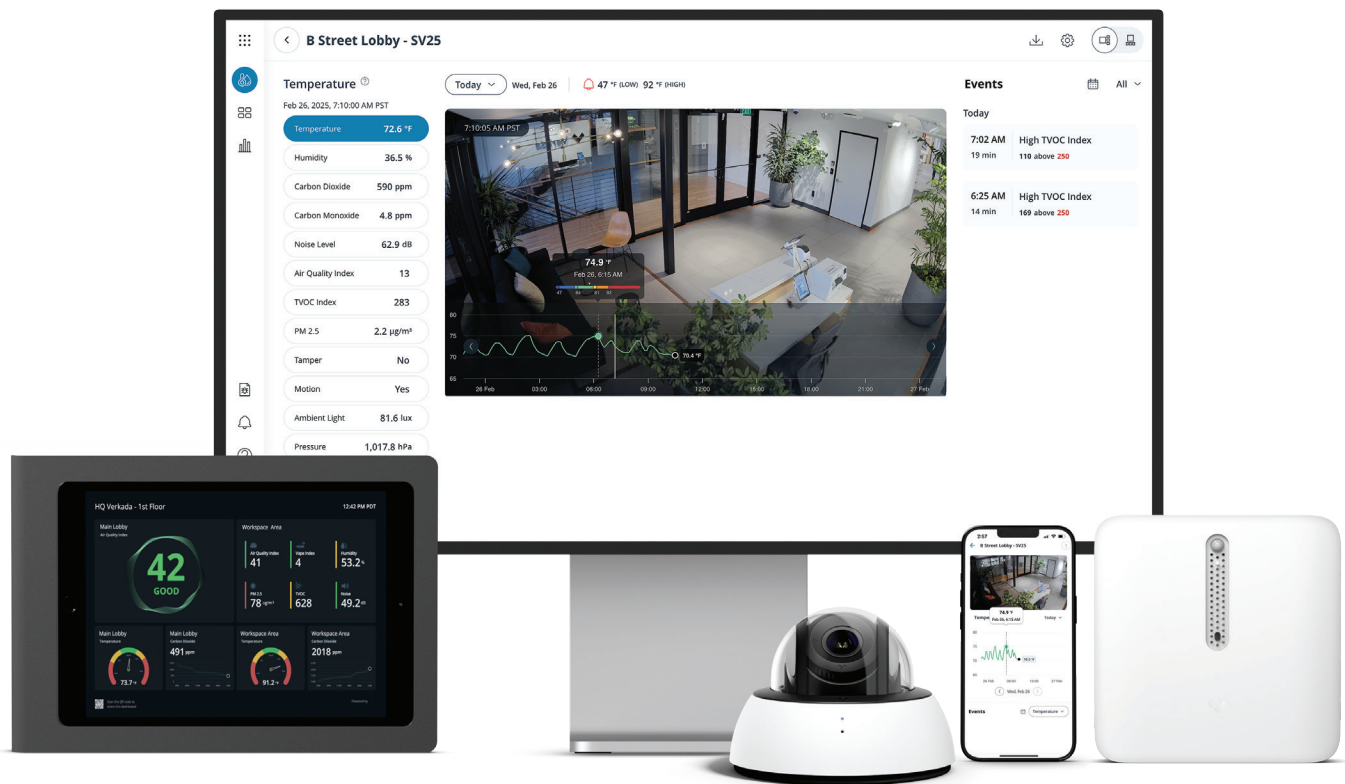
Get notified instantly when conditions in your environment surpass pre-configured thresholds.

## **Visual insights for quick investigations**

Easily monitor air quality and environmental conditions by viewing sensor data across intuitive dashboards.

## **Operational insights and cost savings**

Monitor and analyze operating conditions to spot trends and performance issues resulting from HVAC systems issues, occupancy activity, and more.





# A Sensor for Every Environment

Verkada's SV20 series includes three unique sensors that are designed for distinct use cases. Deploy the ideal air quality sensor in your environment to stay ahead of unseen threats.



Temperature



Vape detection



Formaldehyde



Humidity



PM2.5, PM4.0 & PM10



TVOCs



Carbon dioxide



Tamper



Ambient light



Noise



Motion



Pressure



Air quality index



Carbon monoxide



Audio recording

# Use Cases

Leverage sensor data for a variety of applications across building environments.

## **Vape detection**

Receive alerts when smoking and vaping occurs; pair with public-facing cameras for additional context.

## **Workplace health and safety**

Monitor indoor spaces for changes in indoor air quality conditions such as pollution, allergens, chemicals, and more.

## **OSHA and EPA compliance**

Have a record of being in compliance with regulations (such as noise levels) and reduce the time required for audits.

## **Server room monitoring**

Monitor temperature and humidity in server rooms and IDF closets to protect from equipment malfunction.

## **Mold prevention and food safety**

Measure humidity during hot months to avoid moisture build-up and mold formation.

## **Infrastructure protection**

Monitor particulate matter and AQI readings to determine if HVAC maintenance — such as replacing air filters — is needed.



# Strengthen Security, Simplify Operations

Streamline facility workflows and increase employee safety with Verkada's integrated visitor and mailroom management solutions.

## **Improve the guest experience**

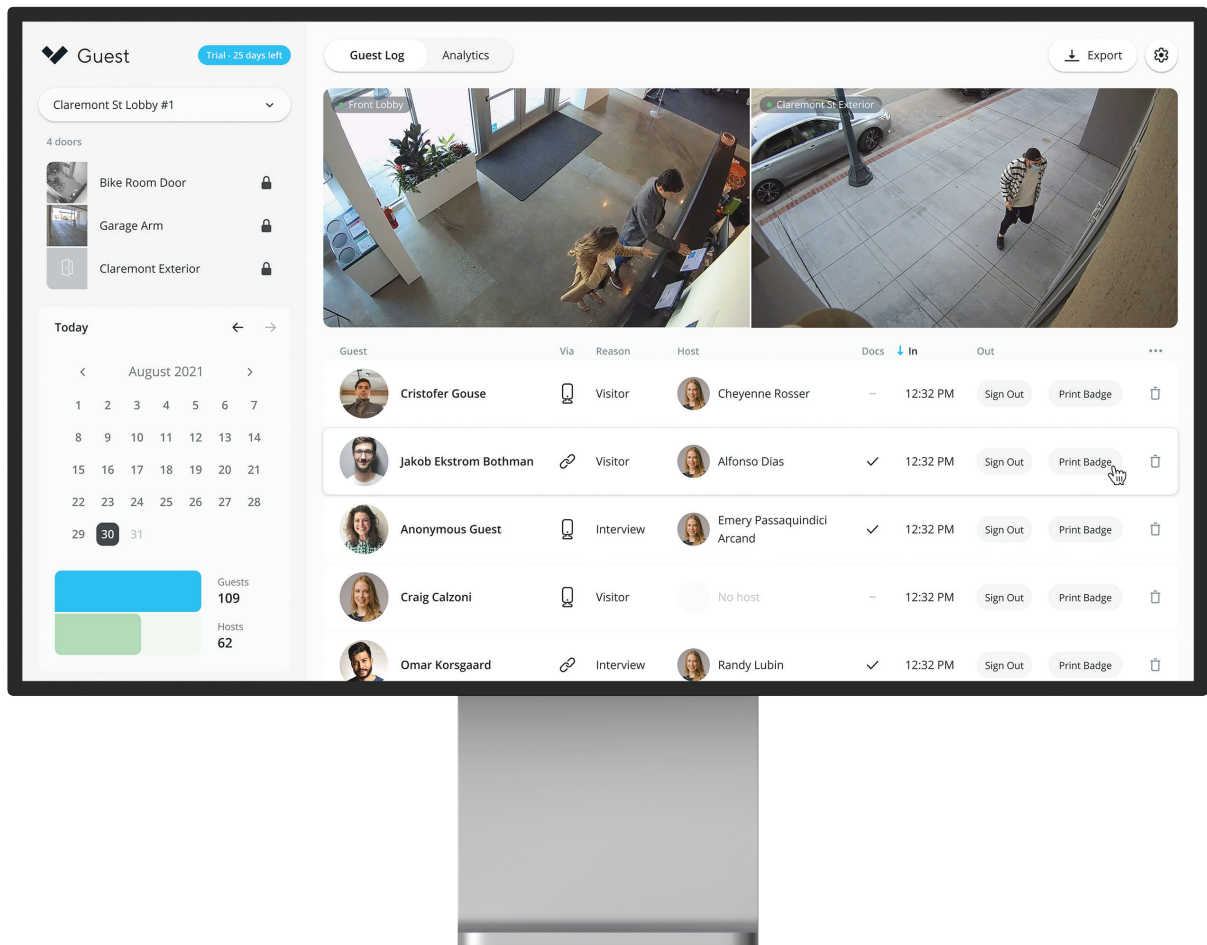
With tailored flows based on visitor type, touchless check-in, instant arrival notifications, and remote unlock, Verkada Guest makes visitors feel welcome the moment they step through the door.

## **Streamline mailroom deliveries**

Reduce manual processes of logging and managing shipments. Easily keep track of inventory, supplies, and deliveries at all times with Verkada Mailroom.

## **Centralize security**

Integrated into the Command platform, Guest and Mailroom work seamlessly with Verkada Cameras and Access Control to provide better visibility and control over your facilities.



“ The integrated view of visitor activity within Command is a game changer. With Guest, we’ve created a safer environment for our teachers and students, while eliminating error-prone logbooks. ”

Meredith Essalat,  
Head of School, Mission Dolores Academy

# Improve Visitor Experience While Strengthening Security

Increase the safety of everyone in your building — employees and guests — and make visitor management a simple, seamless experience.

## **Screen visitors instantly**

Screen visitors against sex offender registries, various criminal databases, and custom deny lists.

## **Centralize security**

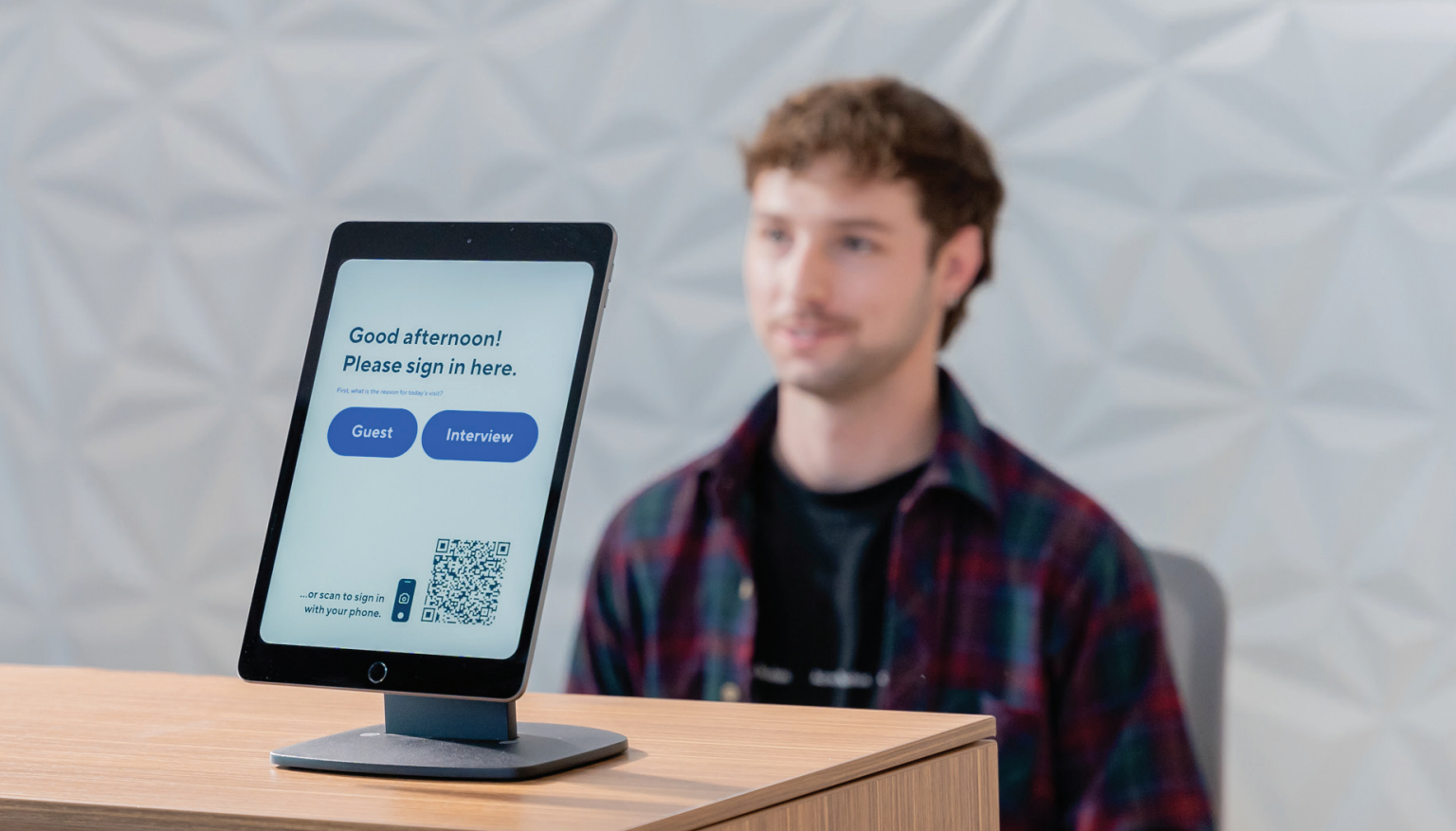
Verkada Guest seamlessly integrates with Video Security and Access Control, making it easy to track arrivals, issue on-demand access credentials, and review visitor activity with linked footage.

## **Set up in minutes**

Simply download the Verkada Guest app and add an iPad and a badge printer to the Command platform. Personalize further with custom branding, guest flows, and site-specific user permissions.

## **Integrate with systems of record**

Simplify admin workflows by integrating with HL7 electronic medical record (EMR) systems and student information systems (SIS).



Integration with  
Verkada Cameras



Integration with  
Verkada Access  
Control



Role-based  
permissions



Customizable  
visitor experience



Touchless  
check-in



Document  
signing



Color badge  
printing



Automatic arrival  
notifications



Analytics and  
reporting



Security  
screening

# Take the Work Out of Mailroom Management

Reduce manual processes of logging and managing deliveries. Simply scan the label on any parcel and Verkada Mailroom will instantly notify the recipient.

## **Streamline mailroom operations**

In just one click, Mailroom scans the shipping label, notifies the recipient, and tracks delivery details in a centralized dashboard.

## **Never miss a package**

Send automated notifications and reminders to employees across Slack, SMS, and email. Plus, help them locate their packages with photos of printed labels.

## **Deter package theft**

With Verkada's camera integration, office managers can easily safeguard assets with a live view of all mailroom activity and a historical snapshot of when the package got scanned.

# Key Features

Protect deliveries at scale with all the features needed to manage mailroom security.



OCR label scanning



Package photo validation



Automatic pickup reminders



Mailroom dashboard



User directory integration



Instant recipient notifications



Filterable search



Verkada camera integration



# Trusted by Organizations Around the World



CANADA GOOSE



EQUINOX



# Try Verkada for Free

Join tens of thousands of organizations worldwide and experience the benefits of Verkada's hybrid cloud system firsthand, at no cost to you.

In just 10 minutes, our devices are online and fully operational. Best of all? Verkada offers unlimited user seats so you can share the benefits of our modern solution with anyone in your organization.

Get started with a free trial by scanning the QR code or visiting **[verkada.com/try](https://verkada.com/try)**

## Your 30-day free trial includes

- Brand-new Verkada device
- 24/7 support via phone, chat, or email
- Full access to Command software
- Pre-paid return shipping label











Get started today  
**[verkada.com/try](https://verkada.com/try)**

## CD63-E Outdoor Dome Camera

### Vivid 4K Coverage in a Variety of Outdoor Environments



#### Overview

The CD63-E outdoor dome camera features a large 1 / 1.2" progressive CMOS image sensor, varifocal lens with 2.25x optical zoom, and 40 meters / 130 feet of IR range to provide unparalleled 4K monitoring in a variety of lighting conditions as well as in inclement weather. The CD63-E includes a powerful CV72S Ambarella processor for advanced analytics like AI-powered search, [Occupancy Trends](#), line crossing, loitering, and Person of Interest (POI) alerts. The CD63-E excels at covering high-traffic exterior environments like building entrances or busy intersections where detailed analytics expedite investigations and provide valuable operational insights.

The CD63-E's robust metal housing, IP66/67 weather rating, and IK10 impact rating enable the device to withstand harsh conditions. Constructed with easy installation top-of-mind, the CD63-E features captive screws that remain attached to the mounting plate, a latch-based cable gland for easy PoE threading, a three-LED light status indicator, and a built-in bubble level to help ensure precise alignment.

#### Key features

##### Superior image quality

- Large 1 / 1.2" progressive CMOS image sensor
- 4K resolution
- Varifocal lens with 2.25x optical zoom
- 40 meters / 130 feet of IR range for optimal nighttime viewing

##### Advanced analytics

- Onboard CV72 Ambarella processor enables people and vehicle analytics
- AI-powered search and AI-powered alerts
- Occupancy Trends for operational insights

##### Durability and weather protection

- Robust metal housing
- IP66/67 weather rating
- IK10 impact rating
- Operability between -40°C to 50°C / -40°F to 122°F

##### Hybrid cloud architecture

- Onboard storage and processing for reduced bandwidth consumption and coverage at scale
- 30 - 120 days (512GB - 3TB) of onboard storage
- Redundant cloud backup and unlimited cloud-based archiving of footage

##### Streamlined installation

- Latch-based cable gland for easy PoE threading
- Captive screws in mounting plate
- Three-LED light status indicator
- Built-in bubble level
- Physical and digital mute switches to easily enable or disable audio



## CD63-E

### Tech Specs

#### Camera features

<b>Image Sensor</b>	1 / 1.2" Progressive CMOS	<b>Shutter Speed</b>	1 / 30 sec. to 1 / 10,000 sec.
<b>Sensor Resolution<sup>1</sup></b>	4K (3840 x 2160)	<b>Day/Night</b>	IR-cut filter for day and night function
<b>Lens Type</b>	Varifocal; motorized zoom	<b>IR Cut Filter</b>	Yes
<b>Focal Length</b>	5.9 - 13.3mm	<b>IR Range</b>	40m / 130ft
<b>Aperture</b>	F1.5 - F2.9	<b>Minimum Illumination</b>	0.009 lux @ F1.9 (Color) 0 lux with IR Illuminators on
<b>Iris</b>	P-Iris	<b>Onboard Storage</b>	Capacity: From 512GB to 3TB Card: MicroSD, SDXC
<b>Field of View (after LDC<sup>2</sup>)</b>	Horizontal: 109° - 49° (102° - 47°) Vertical: 58° - 28° (58° - 27°) Diagonal: 113° - 55° (107° - 53°)	<b>CPU</b>	Ambarella CV72S66
<b>Sensor Movement</b>	Tilt: 65° Pan: 360° Rotation: 350°		

#### Standard video settings

<b>Compression</b>	H.265, H.264	<b>Historical Video Settings</b>	Adaptive quality <sup>1</sup>
<b>Frame Rate<sup>3</sup></b>	24fps	<b>Live Streaming Settings</b>	High quality (HQ): Up to 4,500 Kbps (default) Standard quality (SQ): Up to 600 Kbps

#### Standard audio settings

<b>Audio</b>	Supported	<b>Interface</b>	Built-in microphone
<b>Audio Capacity</b>	One-way audio	<b>Effective Range</b>	5m / 16ft

#### Power and network

<b>Power Input<sup>4</sup></b>	With IR: IEEE 802.3at Type 2 PoE+ Without IR: IEEE 802.3af Type 1 PoE Extended temperature range: IEEE 802.3at Type 2 PoE+	<b>Connectivity</b>	RJ-45 cable connector for network/PoE connection; 10 / 100 / 1000 Mbps
<b>Power Consumption<sup>4</sup></b>	With IR: 43-57V, 0.48-0.36A, 20.4W Without IR: 43-57V, 0.27-0.20A, 11.3W Extended temperature range: 43-57V, 0.60-0.45A, 25.5W	<b>RTSP</b>	RTSP 1.0 RFC 2326 Max concurrent streams: 2 Audio support: Yes

1. All our cameras record in "adaptive quality," capturing both standard (SQ) and high quality (HQ) streams. SQ video is stored up to the amount of retention specified by the customer. The amount of HQ video stored on the camera will depend on the amount of motion detected by the camera over time. To learn more, visit our website: <https://docs.verkada.com/docs/adaptive-quality-recording-whitepaper.pdf>

2. Lens Distortion Correction (LDC) crops the sensor field of view to deliver a rectified, undistorted output image.

3. Frame rate can be adjusted by support.

4. Extended temperature range includes operating temperatures below -10°C / 14°F and assumes IR will be enabled.





# CD63-E

## Tech Specs

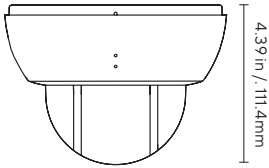
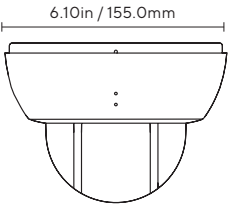
### General

Operating Temperature	-40°C to 50°C / -40°F to 122°F	LED Indicator	System power, status indicator and debug indicator
Humidity	0 to 90%	Warranty	10 Years
Certifications	FCC, ICES, UKCA, CE, RCM, NTRA, NOM, KCC, VCCI, IK10 impact rating, IEC 62368-1, IP66/67 weather rating, Compliant to UL 2043	Included Accessories	Screw packs, mount plate with leveler, cable sealing rubber for 6.5-7.5mm, conduit adapter, T10 security driver, desiccant 4.5g

### Mechanical

Weight	Camera: 1386g / 48.89oz Mount plate: 193g / 6.81oz	Body	Aluminum, plastic dome trim
Dimensions	Ø: 155.0mm / 6.10in, H: 111.4mm / 4.39in with mount plate Ø: 155.0mm / 6.10in, H: 104.4mm / 4.11in without mount plate		

### Dimensions



### Software capabilities

Alerts	Camera status, motion detection, people detection, vehicle detection, Person of Interest detection, crowd detection, line-crossing detection, loitering detection, AI-powered alerts	Streaming and Storage	Cloud backup, configurable retention days, selectable storage location, low bandwidth mode, timelapse, RTSP
People Analytics	People search, attribute search, face search, Occupancy Trends, motion search, trajectory analysis, selective face blurring, AI-powered search	Sharing and Privacy	Live links, live face blur, privacy regions, audit log
Vehicle Analytics	Vehicle search, attribute search, motion search, trajectory analysis, Occupancy Trends, AI-powered search		

## CB62-TE Telephoto Bullet Camera

### Prominent 4K Coverage at Distance in Outdoor Environments



#### Overview

The CB62-TE telephoto bullet camera features a 1 / 2.8" progressive CMOS image sensor, an advanced optical lens with an adjustable focal length of 8mm - 20mm, and powerful long-range IR LEDs (50 meters / 164 feet) for 4K coverage in a variety of lighting and weather conditions. The CB62-TE features an onboard CV22S Ambarella processor for advanced analytics like AI-powered search, [Occupancy Trends](#), line crossing, loitering, and Person of Interest (POI) alerts. The CB62-TE also supports [License Plate Recognition](#) (LPR), enabling it to capture license plates from vehicles traveling up to 80 mph / 128 kph across as many as three lanes of traffic. The CB62-TE excels at covering high-traffic areas of interest such as stadiums and busy parking lot entrances and, because of its telephoto zoom capabilities, provides clear images even when installed far from an area of interest. The CB62-TE is also optimal for reading license plates at distance, and its LPR capabilities can be used to access control gated entrances to facilities.

The CB62-TE is constructed with a robust aluminum unibody and designed to withstand extreme conditions with an IP67 weather rating and IK10 impact rating. The camera's design includes a built-in pigtail connector that expedites PoE cabling by removing the need to disassemble the camera itself. Installation and setup are easy to track using the LED status indicator.

#### Key features

##### Superior image quality

- 1 / 2.8" progressive CMOS image sensor
- 4K resolution
- Varifocal lens with an adjustable focal length of 8mm - 20mm
- 50 meters / 164 feet of IR range for optimal nighttime viewing

##### Advanced analytics

- Onboard CV22S Ambarella processor enables people and vehicle analytics
- License Plate Recognition capabilities capture license plates at speeds up to 80 mph / 128 kph
- AI-powered search and AI-powered alerts
- Occupancy Trends for operational insights

##### Hybrid cloud architecture

- Onboard storage and processing for reduced bandwidth consumption and coverage at scale
- 30 - 90 days (512GB - 2TB) of onboard storage
- Redundant cloud backup and unlimited cloud-based archiving of footage

##### Easy installation

- Built-in pigtail connector for simplified PoE cabling
- Mounting plate and screw pack included
- LED light status indicator

##### Durability and weather protection

- Factory-sealed robust aluminum unibody
- IP67 weather rating
- IK10 impact rating
- Operability between -40°C to 50°C / -40°F to 122°F



## CB62-TE

### Tech Specs

#### Camera features

<b>Image Sensor</b>	1 / 2.8" Progressive CMOS	<b>Shutter Speed</b>	1 / 30 sec. to 1 / 10,000 sec.
<b>Sensor Resolution<sup>1</sup></b>	4K (3840 x 2160)	<b>Day/Night</b>	IR-cut filter for day and night function
<b>Lens Type</b>	Varifocal; motorized zoom	<b>IR Cut Filter</b>	Yes
<b>Focal Length</b>	8mm–20mm	<b>IR Range</b>	50m / 164ft
<b>Aperture</b>	F1.5–F2.8	<b>Minimum Illumination</b>	0.009 lux @ F1.9 (Color) 0 lux with IR Illuminators on
<b>Iris</b>	P-Iris	<b>Onboard Storage</b>	Capacity: From 512GB to 2TB Card: MicroSD, SDXC
<b>Field of View (after LDC<sup>2</sup>)</b>	Horizontal: 42° - 17° (41° - 17°) Vertical: 23° - 9° (23° - 9°) Diagonal: 48° - 19° (46° - 19°)	<b>CPU</b>	Ambarella CV22S66
<b>Camera Movement</b>	Tilt: 0° to 90° Pan: 360° Rotation: 360°		

#### Standard video settings

<b>Compression</b>	H.265, H.264	<b>Historical Video Settings</b>	Adaptive quality <sup>1</sup>
<b>Frame Rate<sup>3</sup></b>	24fps	<b>Live Streaming Settings</b>	High quality (HQ): Up to 4,500 Kbps (default) Standard quality (SQ): Up to 600 Kbps

#### Standard audio settings

<b>Audio</b>	Not supported
--------------	---------------

#### Power and network

<b>Power Input<sup>4</sup></b>	With IR: IEEE 802.3at Type 2 PoE+ Without IR: IEEE 802.3af Type 1 PoE Extended temperature range: IEEE 802.3at Type 2 PoE+	<b>Connectivity</b>	RJ-45 cable connector for network/PoE connection; 10 / 100 Mbps
<b>Power Consumption<sup>4</sup></b>	With IR: 37-57V, 0.40-0.26A, 14.9W Without IR: 37-57V, 0.11-0.08A, 4.3W Extended temperature range: 37-57V, 0.64-0.39A, 23.7W	<b>RTSP</b>	RTSP 1.0 RFC 2326 Max concurrent streams: 2 Audio support: No

1. All our cameras record in "adaptive quality," capturing both standard (SQ) and high quality (HQ) streams. SQ video is stored up to the amount of retention specified by the customer. The amount of HQ video stored on the camera will depend on the amount of motion detected by the camera over time. To learn more, visit our website: <https://docs.verkada.com/docs/adaptive-quality-recording-whitepaper.pdf>

2. Lens Distortion Correction (LDC) crops the sensor field of view to deliver a rectified, undistorted output image.

3. Frame rate can be adjusted by support.

4. Extended temperature range includes operating temperatures below -8.5°C / 16.7°F and assumes IR will be enabled.





# CB62-TE

## Tech Specs

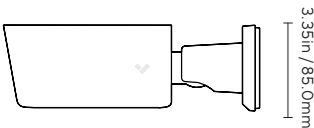
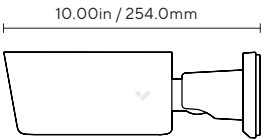
### General

Operating Temperature	-40°C to 50°C / -40°F to 122°F	LED Indicator	System power and status indicator
Humidity	0 to 90%	Warranty	10 Years
Certifications	FCC, ICES, CE, UKCA, RCM, VCCI, KCC, BIS, NOM, CB, UL/cUL/IEC 62368-1, IP67 weather rating, IK10 impact rating, FY2019 NDAA compliant	Included Accessories	4x M4x8 screws, 4x TP4x30 mount screws, mount plate, junction box adapter, junction box cover, T25 hand tool

### Mechanical

Weight	Camera: 1478g / 52.13oz Mount plate: 33g / 1.16oz	Body	Aluminum
Dimensions	Ø: 85.0mm / 3.35in L: 254.0mm / 10.00in		

### Dimensions



### Software capabilities

Alerts	Camera status, motion detection, people detection, vehicle detection, Person of Interest detection, crowd detection, line-crossing detection, loitering detection, AI-powered alerts	Streaming and Storage	Cloud backup, configurable retention days, selectable storage location, low bandwidth mode, timelapse, RTSP
People Analytics	People search, attribute search, face search, Occupancy Trends, motion search, trajectory analysis, selective face blurring, AI-powered search	Sharing and Privacy	Live Links, live face blur, privacy regions, audit log
Vehicle Analytics	Vehicle search, attribute search, motion search, trajectory analysis, Occupancy Trends, AI-powered search	License Plate Recognition	License Plate of Interest alerts, license plate indexing

## CF83-E Fisheye Camera

### Expansive 180° Coverage with Detailed 12.5MP Resolution



#### Overview

The CF83-E fisheye camera features a large 1 / 1.6" progressive CMOS image sensor and 12.5MP resolution for great image quality amid varying lighting conditions and inclement weather. With its onboard CV72S Ambarella processor, the CF83-E delivers advanced analytics like AI-powered search, motion trajectory mapping, line crossing, and loitering alerts. The CF83-E offers wide-angle, 180-degree coverage, yet is built to minimize classic fisheye distortion, making its ePTZ mode particularly effective for live monitoring and clear investigations. The CF83-E is ideal for providing overview coverage of large areas—like city blocks, long corridors, and large interior spaces—all from a single install point.

The CF83-E is built with an in-house industrial design for durability and easy installation. It features a robust metal exterior with an IP66/67 weather rating and IK10 impact protection, ensuring reliable performance in harsh environments. The CF83-E's design streamlines installation and large fleet deployments with features such as captive screws that remain attached to the mounting plate, a latch-based cable gland for easy PoE threading, a three-LED light status indicator, and a built-in bubble level for precise alignment.

#### Key features

##### Excellent image quality

- Large 1 / 1.6" progressive CMOS image sensor
- 12.5MP resolution
- 20 meters / 66 feet of IR range for nighttime viewing

##### Streamlined installation

- Latch-based cable gland for easy PoE threading
- Captive screws in mounting plate
- Three-LED light status indicator
- Built-in bubble level
- Physical and digital mute switches to easily enable or disable audio

##### Advanced analytics

- Onboard CV72S Ambarella processor enables people and vehicle analytics
- AI-powered search and AI-powered alerts

##### Hybrid cloud architecture

- Onboard storage and processing helps reduce bandwidth consumption, and enables coverage at scale
- 30 - 120 days (512GB - 3TB) of onboard storage
- Redundant cloud backup and unlimited cloud-based archiving of footage

##### Durability and weather protection

- Robust metal housing
- IP66/67 weather rating
- IK10 impact rating
- Operability between -40°C to 50°C / -40°F to 122°F

##### Extensive coverage and monitoring

- 180-degree field of view
- ePTZ, panoramic, and split viewing modes for enhanced live monitoring of large areas



## CF83-E

### Tech Specs

#### Camera features

<b>Image Sensor</b>	1 / 1.6" Progressive CMOS	<b>Shutter Speed</b>	1 / 120 sec. to 1 / 32000 sec.
<b>Sensor Resolution<sup>1</sup></b>	12.5MP (3536 x 3536); resolution (3520 x 3520)	<b>Day/Night</b>	IR-cut filter for day and night function
<b>Lens Type</b>	Fixed	<b>IR Cut Filter</b>	Yes
<b>Focal Length</b>	1.7mm	<b>IR Range</b>	20m / 66ft
<b>Aperture</b>	F2.0	<b>Minimum Illumination</b>	0.009 lux @ F1.9 (Color) 0 lux with IR Illuminators on
<b>Iris</b>	Fixed	<b>Onboard Storage</b>	Capacity: From 512GB to 3TB Card: MicroSD, SDXC
<b>Field of View</b>	Horizontal: 180° Vertical: 180° Diagonal: 180°	<b>CPU</b>	Ambarella CV72S66

#### Standard video settings

<b>Compression</b>	H.265, H.264	<b>Historical Video Settings</b>	Adaptive quality <sup>1</sup>
<b>Frame Rate<sup>2</sup></b>	24fps	<b>WDR Technology</b>	120dB dynamic range, true WDR, dual exposure
<b>Live Streaming Settings</b>	High quality (HQ): Up to 4,500 Kbps (default) Standard quality (SQ): Up to 600 Kbps		

#### Standard audio settings

<b>Audio</b>	Supported	<b>Interface</b>	Built-in microphone
<b>Audio Capacity</b>	One-way audio	<b>Effective Range</b>	5m / 16ft

#### Power and network

<b>Power Input<sup>3</sup></b>	With IR: IEEE 802.3at Type 2 PoE+ Extended temperature range: IEEE 802.3at Type 2 PoE+	<b>Connectivity</b>	RJ-45 cable connector for network/ PoE connection; 10 / 100 / 1000 Mbps
<b>Power Consumption<sup>3</sup></b>	With IR: 43-57V, 0.46-0.34A, 19.5W Without IR: 43-57V, 0.22-0.17A, 9.5W Extended temperature range: 43-57V, 0.58-0.44A, 24.8W	<b>RTSP</b>	RTSP 1.0 RFC 2326 Max concurrent streams: 2 Audio support: No

1. All our cameras record in "adaptive quality," capturing both standard (SQ) and high quality (HQ) streams. SQ video is stored up to the amount of retention specified by the customer. The amount of HQ video stored on the camera will depend on the amount of motion detected by the camera over time. To learn more, visit our website:

<https://docs.verkada.com/docs/adaptive-quality-recording-whitepaper.pdf>

2. Frame rate can be adjusted by support.

3. Extended temperature range includes operating temperatures below -8.5°C / 16.7°F and assumes IR will be enabled.



# CF83-E

## Tech Specs

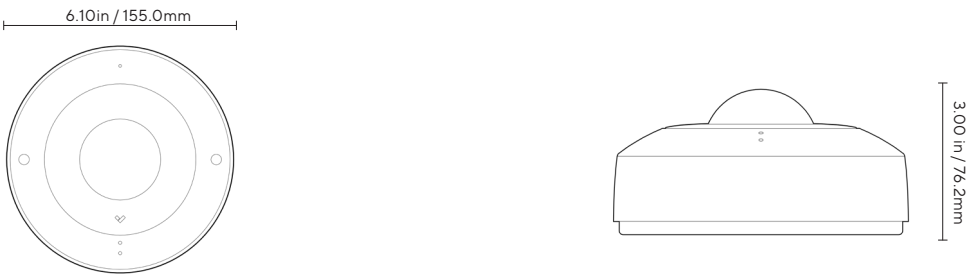
### General

Operating Temperature	-40°C to 50°C / -40°F to 122°F	LED Indicator	System power, status indicator, and debug indicator
Humidity	0 to 90%	Warranty	10 Years
Certifications	FCC, ICES, CE, UKCA, VCCI, NOM, NTRA, KCC, UL/cUL/IEC 62368-1, IK10 impact rating, ICASA, IP66/67 weather rating	Included Accessories	Screw packs, mount plate with leveler, cable sealing rubber for 6.5-7.5mm, conduit adapter, T10 security driver

### Mechanical

Weight	Camera: 1368g / 48.25oz Mount plate: 196g / 6.91oz	Body	Aluminum, plastic dome trim
Dimensions	Ø: 155.0mm / 6.10in, H: 76.2mm / 3.00in with mount plate Ø: 155.0mm / 6.10in, H: 69.2mm / 2.72in without mount plate		

### Dimensions



### Software capabilities

Alerts	Camera status, motion detection, people detection, vehicle detection, Person of Interest detection, crowd detection, AI-powered alerts	Streaming and Storage	Cloud backup, configurable retention days, selectable storage location, low bandwidth mode, timelapse, RTSP
People Analytics	People search, attribute search, face search, motion search, trajectory analysis <sup>4</sup> , selective face blurring, AI-powered search	Sharing and Privacy	Live links, privacy regions, audit log
Vehicle Analytics	Vehicle search, attribute search, motion search, trajectory analysis <sup>4</sup> , AI-powered search		

4. Trajectory analysis is supported in four-way split, panoramic, and ePTZ circle mode.

## CH52-E Multisensor Camera

# 20MP of Detailed Coverage From a Single Install Point



## Overview

The CH52-E multisensor camera features four independent sensors, providing expansive coverage from a single install point. Each sensor includes a 1 / 2.8" progressive CMOS image sensor, varifocal lens with 2.08x optical zoom, and 30 meters / 98 feet of IR range to provide clear and consistent image quality in any lighting condition. The CH52-E includes four onboard CV25S Ambarella processors to support advanced analytics like AI-powered search, [Occupancy Trends](#), line crossing, loitering, and Person of Interest (POI) alerts. The CH52-E excels at covering hallway intersections and exterior corners of buildings, providing comprehensive visibility and eliminating blind spots while only requiring a single PoE++ cable.

With sealed interior components and IP66 weather and IK10 impact ratings, the CH52-E withstands extreme temperatures and excessive precipitation, allowing it to be deployed in a variety of interior or exterior environments. Installation and setup are easy to track using the LED status indicator, while the need for a single cable run minimizes port use.

## Key features

### Excellent image quality

- Four 1 / 2.8" progressive CMOS image sensors
- 20MP (4 x 5MP) of collective resolution
- Four varifocal lenses with 2.08x optical zoom each
- 30 meters / 98 feet of IR range for nighttime viewing

### Expansive coverage

- Individually adjustable and repositionable sensor heads
- Combined field of view up to 328°

### Advanced analytics

- Four onboard CV25S Ambarella processors enable people and vehicle analytics
- AI-powered search and AI-powered alerts
- Occupancy Trends for operational insights

### Durability and weather protection

- Sealed interior components
- IP66 weather rating
- IK10 impact rating
- Operability between -40°C to 50°C / -40°F to 122°F

### Hybrid cloud architecture

- Onboard storage and processing for reduced bandwidth consumption and coverage at scale
- 30 - 365 days (1TB - 8TB) of onboard storage
- Redundant cloud backup and unlimited cloud-based archiving of footage

### Easy installation

- Single PoE++ cable required
- Mounting template and screws included
- LED light status indicator



## CH52-E

### Tech Specs

#### Camera features

<b>Image Sensor</b>	4 x 1 / 2.8" Progressive CMOS	<b>Shutter Speed</b>	1 / 5 sec. to 1 / 32,000 sec.
<b>Sensor Resolution<sup>1</sup></b>	4 x 5MP (2688 x 1944)	<b>Day/Night</b>	IR-cut filter for day and night function
<b>Lens Type</b>	Varifocal; motorized zoom	<b>IR Cut Filter</b>	Yes
<b>Focal Length</b>	3.7-7.7mm	<b>IR Range</b>	30m / 98ft; non-adjustable
<b>Aperture</b>	F1.9 - F2.9	<b>Minimum Illumination</b>	0.009 lux @ F1.9 (color) 0 lux with IR Illuminators on
<b>Iris</b>	N/A	<b>Onboard Storage</b>	Capacity: From 1TB to 8TB Card: MicroSD, SDXC
<b>Field of View (after LDC<sup>2</sup>)</b>	Horizontal: 89° - 37° (82° - 35°) Vertical: 65° - 29° (60° - 26°) Diagonal: 99° - 46° (92° - 43°)	<b>CPU</b>	4 x Ambarella CV25S88
<b>Sensor Movement</b>	Tilt: +0°-105° for each lens from horizon Pan: +/- 90° for each lens Rotation: +/- 90° for each lens		

#### Standard video settings

<b>Compression</b>	H.265, H.264	<b>Historical Video Settings</b>	Adaptive quality <sup>1</sup>
<b>Frame Rate<sup>3</sup></b>	24fps / sensor	<b>WDR Technology</b>	120dB dynamic range, true WDR, dual exposure
<b>Live Streaming Settings (Per Head)</b>	High quality (HQ): Up to 3,000 Kbps (default) Standard quality (SQ): Up to 600 Kbps		

#### Standard audio settings

<b>Audio</b>	Not supported
--------------	---------------

#### Power and network

<b>Power Input<sup>4</sup></b>	With IR: IEEE 802.3bt Type 3 PoE++ Without IR: IEEE 802.3at Type 2 PoE+ Extended temperature range: IEEE 802.3bt Type 3 PoE++	<b>Connectivity</b>	RJ-45 cable connector for network/PoE connection; 10 / 100 Mbps
<b>Power Consumption<sup>4</sup></b>	With IR: 43-57V, 0.65-0.49A, 27.7W Without IR: 43-57V, 0.46-0.34A, 19.5W Extended temperature range: 43-57V, 0.91-0.68A, 38.7W	<b>RTSP</b>	RTSP 1.0 RFC 2326 Max concurrent streams: 8 (2 per camera head) Audio support: No

1. All our cameras record in "adaptive quality," capturing both standard (SQ) and high quality (HQ) streams. SQ video is stored up to the amount of retention specified by the customer. The amount of HQ video stored on the camera will depend on the amount of motion detected by the camera over time. To learn more, visit our website: <https://docs.verkada.com/docs/adaptive-quality-recording-whitepaper.pdf>

2. Lens Distortion Correction (LDC) crops the sensor field of view to deliver a rectified, undistorted output image.

3. Frame rate can be adjusted by support.

4. Extended temperature range includes operating temperatures below -8.5°C / 16.7°F and assumes IR will be enabled.



## CH52-E

### Tech Specs

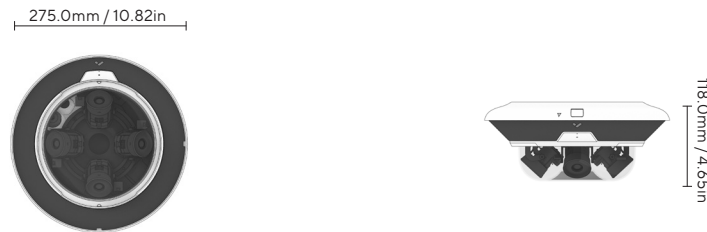
#### General

<b>Operating Temperature</b>	-40°C to 50°C / -40°F to 122°F	<b>LED Indicator</b>	System power and status indicator
<b>Humidity</b>	0 to 90%	<b>Warranty</b>	10 Years
<b>Certifications</b>	FCC, ICES, CE, UKCA, RCM, VCCI, KCC, NOM, CB, NTRA, ICASA, UL/cUL/IEC 62368-1, IK10 impact rating, IP66 weather rating, FY2019 NDAA compliant	<b>Included Accessories</b>	IR cover, mounting template, 3 mounting screws, 3 wall anchors, 2 desiccants, T10 security screwdriver, offset wrench

#### Mechanical

<b>Weight</b>	Camera: 2,900g / 102.29oz Mount plate: 536g / 18.91oz	<b>Body</b>	Aluminum, plastic dome trim
<b>Dimensions</b>	Ø: 275.0mm / 10.82in, H: 118.0mm / 4.65in with mount plate Ø: 267.0mm / 10.51in, H: 114.0mm / 4.49in without mount plate		

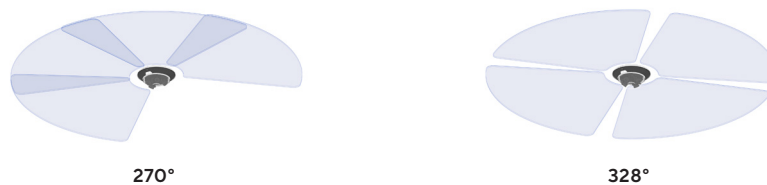
#### Dimensions



#### Software capabilities

<b>Alerts<sup>5</sup></b>	Camera status, motion detection, people detection, vehicle detection, Person of Interest detection, crowd detection, line-crossing detection, loitering detection, AI-powered alerts	<b>Streaming and Storage<sup>5</sup></b>	Cloud backup, configurable retention days, selectable storage location, low bandwidth mode, timelapse, RTSP
<b>People Analytics<sup>5</sup></b>	People search, attribute search, face search, Occupancy Trends, motion search, trajectory analysis, selective face blurring, AI-powered search	<b>Sharing and Privacy<sup>5</sup></b>	Live Links, live face blur, privacy regions, audit log
<b>Vehicle Analytics<sup>5</sup></b>	Vehicle search, attribute search, motion search, trajectory analysis, Occupancy Trends, AI-powered search		

#### Coverage examples



5. All the listed features can be enabled independently for each camera head.

## CP63-E PTZ Camera

4K PTZ for Expansive and Highly-Detailed Coverage of Large Areas



## Overview

The CP63-E 4K PTZ camera includes a large 1 / 1.8" progressive CMOS image sensor for superior image quality and precise, detailed monitoring. The CP63-E's advanced varifocal lens with 32x motorized optical zoom and 100-meter IR range complement its Sentry Mode for unparalleled, automated monitoring of individuals across an expansive field of view. With its onboard CV72S Ambarella processor delivering advanced analytics like AI-powered search, AI-powered alerts, Person of Interest detection, and crowd detection, the CP63-E excels in monitoring large areas such as sports fields, parking lots, or stadiums.

## Key features

### Superior image quality

- Large 1 / 1.8" progressive CMOS image sensor
- 4K resolution
- Varifocal lens with 32x optical zoom
- 100 meters / 328 feet of IR range for long-range nighttime viewing

### Advanced analytics

- Onboard CV72S Ambarella processor enables people and vehicle analytics
- AI-powered search and AI-powered alerts

### Automated monitoring

- Support Sentry Mode with up to three context cameras for automated monitoring of vast areas

### Hybrid cloud architecture

- Onboard storage and processing helps reduce bandwidth consumption, enabling coverage at scale
- 30 - 90 days (1TB - 3TB) of onboard storage
- Redundant cloud backup and unlimited cloud-based archiving of footage monitoring

### Durability and weather protection

- Robust metal housing
- IP66 weather rating
- IK10 impact rating
- Operability between -40°C to 50°C / -40°F to 122°F





## CP63-E

### Tech Specs

#### Camera features

<b>Image Sensor</b>	1 / 1.8" Progressive CMOS	<b>Shutter Speed</b>	1 / 30 sec. to 1 / 10,000 sec.
<b>Sensor Resolution<sup>1</sup></b>	4K (3840 x 2160)	<b>Day/Night</b>	IR-cut filter for day and night function
<b>Lens Type</b>	Varifocal; motorized zoom	<b>IR Cut Filter</b>	Yes
<b>Focal Length</b>	6.5mm – 212mm	<b>IR Range</b>	100m / 328ft
<b>Aperture</b>	F1.4 – F4.9	<b>Minimum Illumination</b>	0.02 lux @ F1.4 (Color) 0 lux @ F1.4 with IR Illuminators on
<b>Iris</b>	P-Iris	<b>Onboard Storage</b>	Capacity: from 1TB to 3TB Card: MicroSD, SDXC
<b>Field of View</b>	Horizontal: 64° - 2° Vertical: 37° - 1° Diagonal: 71° - 2°	<b>CPU</b>	Ambarella CV72S66
<b>Sensor Movement</b>	Tilt: 220° Pan: 360°		

#### Standard video settings

<b>Compression</b>	H.265 (historical video only), H.264	<b>Historical Video Settings</b>	Adaptive quality <sup>1</sup>
<b>Frame Rate<sup>2</sup></b>	24fps	<b>WDR Technology</b>	True WDR, dual exposure
<b>Live Streaming Settings<sup>3</sup></b>	Static: 1,000 Kbps (SQ), 3,000 Kbps (HQ) Moving: 3,000 Kbps (SQ), 5,000 Kbps (HQ)		

#### Standard audio settings

<b>Audio</b>	Not supported
--------------	---------------

#### Power and network

<b>Power Input<sup>4</sup></b>	With IR: IEEE 802.3bt Type 3 PoE++ Without IR: IEEE 802.3bt Type 3 PoE++ Extended temperature range: IEEE 802.3bt Type 3 PoE++	<b>Connectivity</b>	RJ-45 cable connector for network/PoE connection; 10 / 100 / 1000 Mbps
<b>Power Consumption<sup>4</sup></b>	With IR: 43-57V, 1.13-0.85A, 48.0W Without IR: 43-57V, 0.80-0.60A, 34.0W Extended temperature range: 43-57V, 1.20-0.89A, 51.0W	<b>RTSP</b>	RTSP 1.0 RFC 2326 Max concurrent streams: 2 Audio support: No

1. All our cameras record in "adaptive quality," capturing both standard (SQ) and high quality (HQ) streams. SQ video is stored up to the amount of retention specified by the customer. The amount of HQ video stored on the camera will depend on the amount of motion detected by the camera over time. To learn more, visit our website:

<https://docs.verkada.com/docs/adaptive-quality-recording-whitepaper.pdf>

2. Frame rate can be adjusted by support.

3. The listed ranges represent the uplink bandwidth based on target bitrates. To learn more, visit Verkada's Knowledge Base and read "[Understanding Variable Bitrates for Verkada PTZ Cameras](#)".

4. Extended temperature range includes operating temperatures below -8.5°C / 16.7°F and assumes IR will be enabled.



## CP63-E

### Tech Specs

#### General

<b>Operating Temperature</b>	-40°C to 50°C / -40°F to 122°F	<b>LED Indicator</b>	System power and status indicator
<b>Humidity</b>	0 to 90%	<b>Warranty</b>	5 Years
<b>Certifications</b>	FCC, IC, CE, UKCA, RCM, VCCI, NOM, IK10 impact rating, IP66 weather rating	<b>Included Accessories</b>	Rubber cap, pendant cap, T30 security L-wrench

#### Mechanical

<b>Weight</b>	Camera: 7.53kg / 16.6lbs Pendant cap: 0.41kg / 0.9lbs	<b>Body</b>	Aluminum, plastic, glass
<b>Dimensions</b>	Ø: 256.0mm / 10.08in, H: 406.0mm / 15.98in with pendant cap Ø: 256.0mm / 10.08in, H: 336.0mm / 13.23in without pendant cap		

#### Dimensions

256.0mm / 10.08in



406.0mm / 15.98in

#### Software capabilities

<b>Alerts</b>	Camera status, motion detection, people detection, vehicle detection, Person of Interest detection, crowd detection, AI-powered alerts	<b>Streaming and Storage</b>	Cloud backup, configurable retention days, selectable storage location, low bandwidth mode, timelapse, RTSP, footage archiving
<b>People Analytics</b>	People search, attribute search, face search, Sentry Mode, motion search, trajectory analysis, selective face blurring, AI-powered search	<b>Sharing and Privacy</b>	Live links, audit log
<b>Vehicle Analytics</b>	Vehicle search, attribute search, motion search, trajectory analysis, AI-powered search	<b>Controllers<sup>5</sup></b>	Mouse, keyboard, Xbox Wireless Controller, joystick

#### Coverage examples



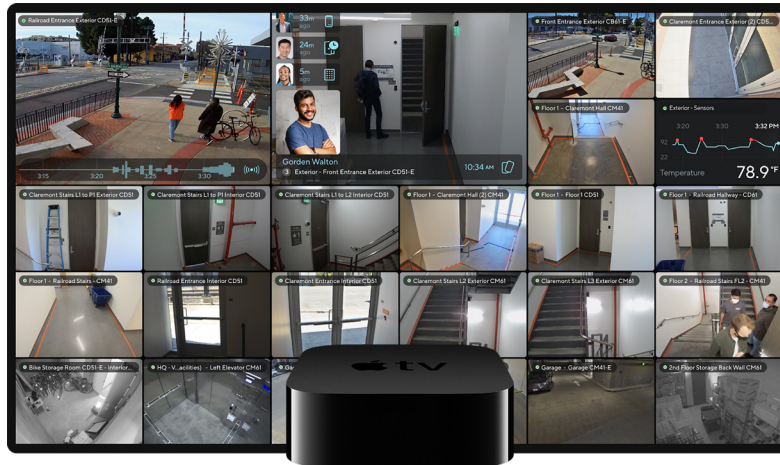
360° pan



220° tilt

5. For details on the supported controllers for the CP63-E, refer to the article [here](#).

## Optimized for Live Viewing



### Overview

The VX52 is a dedicated device that streams up to 300 camera feeds (30 cameras per page, up to 10 pages) to any display with ultra-low latency, crisp video playback, customizable Smart Tiles and layouts. Built on the powerful Apple TV 4K platform, the VX52 is the viewing platform of choice for customers with mission-critical real-time viewing requirements.

#### Administrator managed device

Admins can remotely manage the VX52, select video feeds and Smart Tiles to display as well as customize layouts. Non-admin viewers do not need accounts, cannot access historical footage and cannot modify display settings.

#### Plug-and-play by design

Simply connect the device to your network via ethernet or wifi and project on a display. The VX52 is ready to stream in minutes with zero configuration needed.

#### Stable and resilient

Streams play continuously without interruption for both local and remote streaming. There is no need to reset the device or relaunch a browser or application — streams restart automatically after a power outage.

#### Supported by Verkada

Admins configure the VX52 in Command, just like their cameras. The VX52 is backed by our industry-leading 10-year warranty and the dedicated Verkada customer support team.

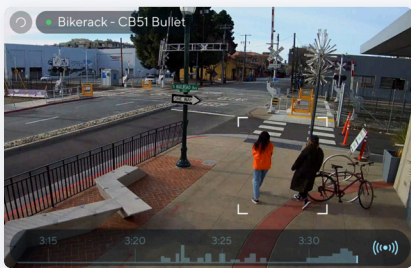
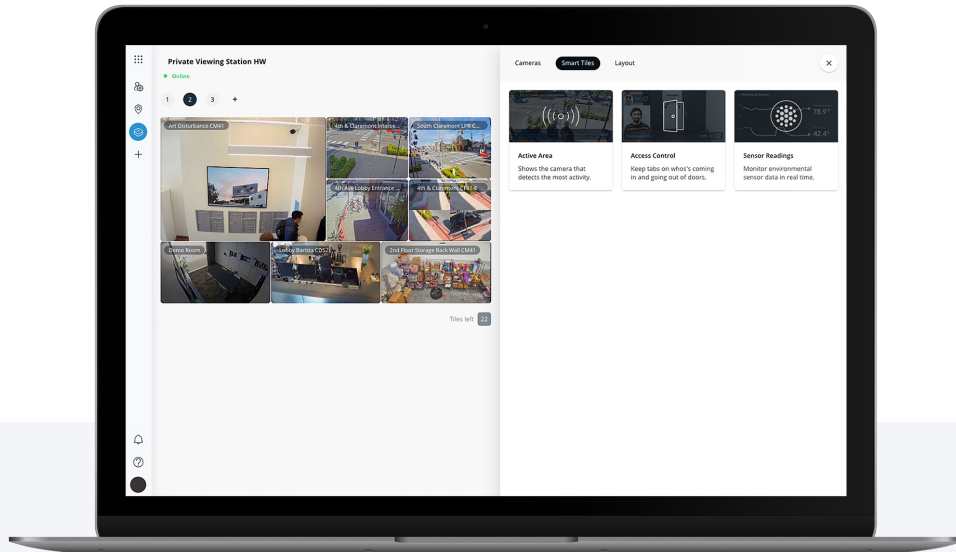
### Key features

- Stream up to 300 cameras across 10 pages on a single display
- Ultra-low latency with crisp video playback
- Administrator managed device without requiring additional accounts
- Plug-and-play with zero local configuration needed
- Easily configure Smart Tiles and layout display from Command
- Automatically restarts after a power outage
- 10-year warranty



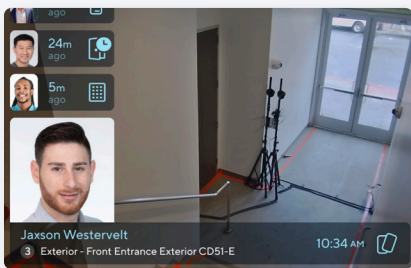
## Smart Tiles

Easily configure your video wall using Smart Tiles from Command to prioritize camera feeds with high motion activity, door access control events and environmental data in real-time.



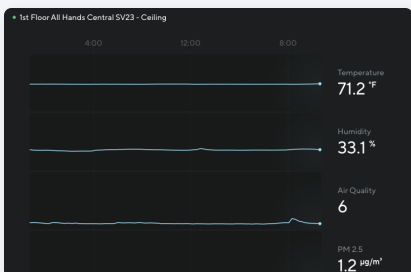
### Active area

The active area tile allows customers to see the camera which has the most motion. This tile will dynamically switch to the camera that has the most motion in its field of view automatically. This is great for users to easily see where in their facility activity is happening and decide if it is something they need to act upon. There is also a graph at the bottom that shows over time when motion was detected the most.



### Access Control

The Access Control tile shows customers a live list of Access events alongside the camera feed of that event. Door events (opens, Door Held Opens, Door Forced Opens) and badge ins show in a feed with the corresponding camera footage. Customers can quickly see when their employees are going through the building.

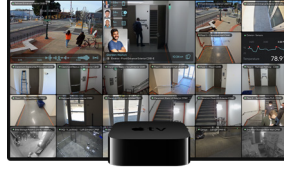


### Air Quality

The Sensor tile shows customers the current readings of their sensor deployment. Each tile is assigned to a specific sensor and customers can configure which readings to show on each tile. Customers can see if any of their sensors' readings are abnormal at a glance to make sure they are on top of their facility.



## Viewing Station Tech Specs

**VX52**

### Viewing Station features

<b>Supported Displays</b>	One display per station	<b>Number of Streams</b>	Up to 300 cameras (local and remote); 30 per page
<b>Supported Resolution</b>	Up to 4096 x 2160 resolution	<b>CPU</b>	A12 Bionic chip with 64-bit architecture

### Power and network

<b>Connectivity</b>	RJ-45 cable connector; 10/100/1000 Mbps	<b>Wifi Connectivity</b>	802.11ax WiFi 6 with MIMO
<b>Connectors</b>	HDMI 2.1 port, gigabit ethernet		

### General

<b>Operating Temperature</b>	0°C to 35°C / 32°F to 95°F	<b>Humidity</b>	0 to 95%
<b>Storage Temperature</b>	-20°C to 45°C / -4°F to 113°F	<b>Warranty</b>	10 Years
<b>Operating Altitude</b>	Up to 3000m / 10,000ft	<b>Included Accessories</b>	HDMI cord, setup guide, power cord, Apple TV remote

### Mechanical

<b>Weight</b>	425g / 15oz	<b>Body</b>	Recycled aluminum and plastic
<b>Dimensions</b>	H: 35.6mm / 1.4in L: 99.1mm / 3.9in W: 99.1mm / 3.9in		

## GC31 Cellular Gateway

### Connect Any Verkada Device, Anywhere



## Overview

The GC31 and GC31-E Cellular Gateways make it simple to deploy Verkada products anywhere with power and cell signal, including hard-to-wire locations such as parking lots, construction sites, or streetlight poles.

Simply feed the GC31 any power input and it will send both power and data to any Verkada device via PoE. Like all Verkada products, the GC31 is cloud-managed and natively integrates with other devices in our ecosystem. And with Verkada's unlimited data plan, which works out-of-the-box in many countries throughout the world, customers no longer need to work with cell carriers.

## Key features

### Flexible power options

Use any power input, including terminal block, barrel jack, and PoE. The gateway has two PoE outputs that provide up to 60W total.

### Verkada data plan or BYO plan

Eliminate complexity with the Verkada data plan or bring your own plan. The Verkada plan offers truly unlimited data, multi-carrier redundancy, and 24/7 support.

### Deploy anywhere

The GC31 comes in both indoor and outdoor versions that cover almost any environment and installation scenario, including pole, roof, wall, and tabletop.

### Cloud-managed

Set up and manage the GC31 in Verkada Command from any device and any location. See all your gateways on a map, run diagnostics, and receive alerts if connectivity is lost.

### Remote troubleshooting

Remotely power cycle the GC31 and any connected devices via Command. If the gateway itself is offline, it will automatically power cycle itself after 30 minutes.

### Optimized data usage

The GC31 optimizes streaming, cloud backup, and other activities on downstream Verkada devices to reduce data usage and improve the viewing experience.





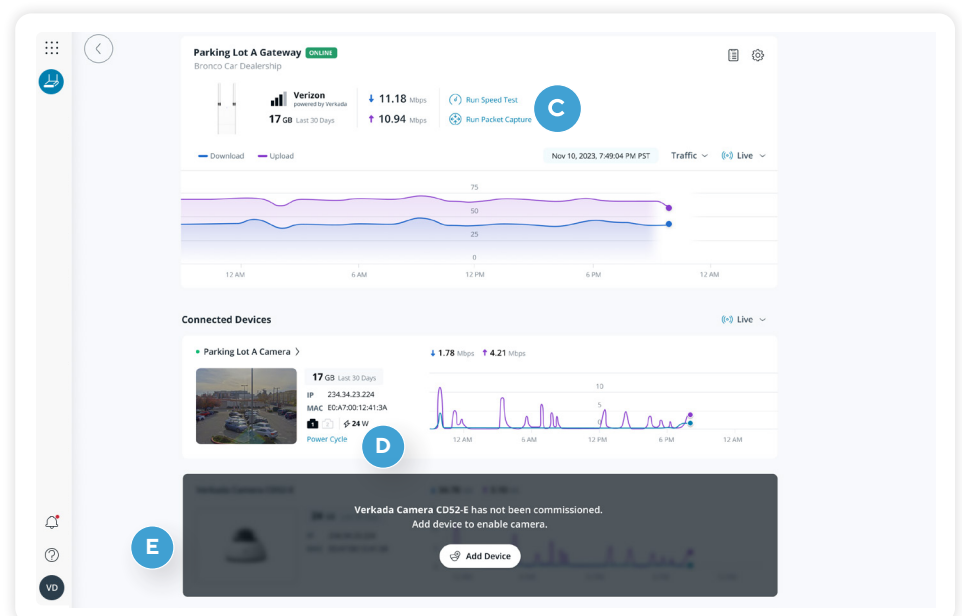
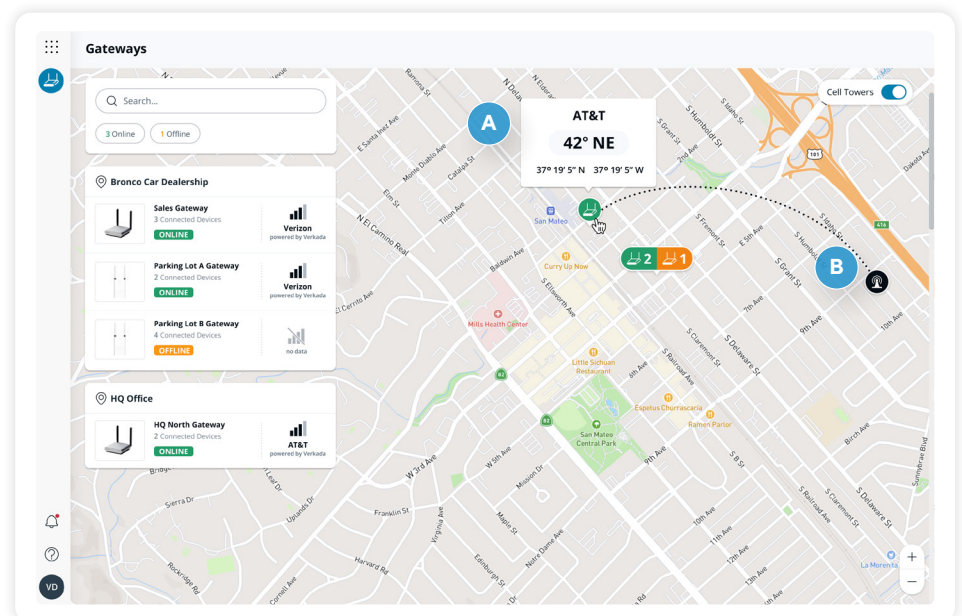
## Deploy anywhere

The Verkada Cellular Gateway comes in both indoor and outdoor versions that cover a wide range of installation scenarios. The GC31-E outdoor model is IP66 rated and can be easily mounted on a pole, wall or roof. The GC31 indoor model can be wall mounted or secured on a tabletop using the Kensington lock.



## Manage from anywhere

- A. View the status and GPS location of your gateways
- B. See which cell tower each gateway is using
- C. Remotely run packet capture and speed tests
- D. Remotely power cycle devices
- E. Recognize connected Verkada devices and streamline setup





## Verkada Data Plan

Verkada takes away the challenge of working with cell carriers with our hassle-free data plan, which works out of the box in many countries across the world.

### Key benefits

#### Instant connectivity out of the box

As soon as it receives power, the GC31 will automatically connect to a carrier using the pre-inserted Verkada SIM card – it just works.

#### Unlimited data

Unlike most carriers, which throttle your speed after a certain threshold, Verkada offers truly unlimited data.

#### Global coverage

The table below shows which carriers we currently use in each country that we support. In the US, the Verkada SIM will default to Verizon and failover to AT&T or T-Mobile if needed.

Country/region	Carriers used
US	Verizon, AT&T, T-Mobile
Canada	Telus, Rogers
UK	O2, Three, EE, Vodafone
Australia	Optus, Telstra
European Union	<a href="#">See full list</a>

### How it works

The base cloud license for the GC31 already includes unlimited data for Verkada non-video devices, such as access controllers or sensors. Unlimited data for Verkada video devices, such as cameras or intercoms, can be purchased through an add-on data license. Please see Ordering Information at the end of this document for pricing.

Note: Cloud backup is disabled on devices that use the Verkada data plan. Customers can enable cloud backup if they bring their own data plan. For more details, please refer to this [knowledge base article](#).

## Bring Your Own Data Plan

Customers also have the option to bring their own data plan. The GC31 is compatible with SIM cards from virtually all major carriers in most countries throughout the world. For a list of carriers that have been tested and verified by Verkada, please refer to this [knowledge base article](#).

#### Always connected

Customers can insert their own SIM card in one slot while keeping the Verkada SIM in the other slot for automatic failover. If the customer-provided SIM fails, the Verkada SIM helps ensure that the gateway is always reachable.

#### Flexible configuration

Customers may also use their own SIM cards in both slots. In this case, customers can configure one slot as the primary SIM and use the other for automatic failover if needed.





## GC31 Tech Specs



### GC31 Indoor Cellular Gateway

#### Cellular

<b>Connectivity</b>	LTE cellular CAT 12	<b>MIMO</b>	2x2 DL MIMO
<b>SIM</b>	2 SIM slots (Nano 4FF) Dual SIM/auto SIM failover	<b>Bands</b>	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B38, B39, B40, B41, B42, B43, B48 (CBRS), B66, B71
<b>Antennas</b>	2 x external omni (SMA)		

#### Inputs and outputs

<b>Ethernet</b>	2 x GigE RJ45 ports (1 x LAN and 1 x WAN/LAN configurable)	<b>Power Output</b>	2 x 802.3bt PoE++ capable ports 60W total power budget
<b>Power Input</b>	54V DC Barrel Jack (6.5/3.0mm OD/ID) 100-240V AC/DC power adapter included (region specific)	<b>GNSS/GPS</b>	Passive GNSS (GPS, GLONASS, and Galileo)

#### Compliance and certifications

<b>RF &amp; EMC</b>	FCC, IC, CE, UKCA, RCM, NOM, VCCI	<b>Cellular<sup>1</sup></b>	PTCRB, GCF, Verizon, T-Mobile, AT&T, FirstNet
<b>Safety</b>	UL/IEC 62368-1, CSA C22.2 No. 62368-1		

#### General

<b>Power Consumption</b>	9W Note: Does not include connected devices	<b>Weight</b>	0.6kg / 1.3lbs
<b>Operating Temperature</b>	-10°C to 50°C / 14°F to 122°F	<b>LEDs</b>	1 status LED, 2 SIM indicator LEDs, 4 signal strength LEDs
<b>Humidity</b>	5-90% RH non-condensing	<b>Warranty</b>	10 years
<b>Dimensions</b>	Main Unit: L: 125mm / 4.9in W: 125mm / 4.9in H: 30mm / 1.2in Antenna: L: 20mm / 0.8in W: 10mm / 0.4in H: 136mm / 5.4in	<b>Included Accessories</b>	2 x SMA antennas, AC/DC power adapter and cord, mount plate, 4 x wall anchors, T10 security torx screwdriver, 4 M4 x 25mm PH2 wall screws, RJ45 port cover
<b>Mounting Options</b>	Wall mount or tabletop (with Kensington slot)		

1. Cellular carriers and operators throughout the world may only require telecom industry certifications such as PTCRB to operate on their network. Some carriers require additional testing and approval, beyond telecom certifications. A carrier listed in the approvals section means Verkada completed additional testing and acquired technical approval for that given carrier. Any carrier not listed may not require additional testing or approval beyond telecom industry certifications to operate on their network.



## GC31 Indoor Cellular Gateway

### Inputs and Outputs





## GC31-E Tech Specs



### GC31-E Outdoor Cellular Gateway

#### Cellular

<b>Connectivity</b>	LTE cellular CAT 12	<b>MIMO</b>	2x2 DL MIMO
<b>SIM</b>	2 SIM slots (Nano 4FF) Dual SIM/auto SIM failover	<b>Bands</b>	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B38, B39, B40, B41, B42, B43, B48 (CBRS), B66, B71
<b>Antennas</b>	2 x external omni (N-type male)		

#### Inputs and outputs

<b>Ethernet</b>	3 x GigE RJ45 ports (2 x LAN and 1 x WAN/LAN configurable)	<b>Power Output</b>	2 x 802.3bt PoE++ capable ports 60W total power budget
<b>Power Input</b>	54V DC Barrel Jack (6.5/3.0mm OD/ID) IEEE 802.3bt Type 4 PoE++ 90W 12-36V DC Terminal Block	<b>GNSS/GPS</b>	Passive GNSS (GPS, GLONASS, and Galileo)

#### Compliance and certifications

<b>RF &amp; EMC</b>	FCC, IC, CE, UKCA, RCM, NOM, VCCI	<b>Cellular<sup>1</sup></b>	PTCRB, GCF, Verizon, T-Mobile, AT&T, FirstNet
<b>Safety</b>	UL/IEC 62368-1, CSA C22.2 No. 62368-1	<b>Weather Rating</b>	IP66

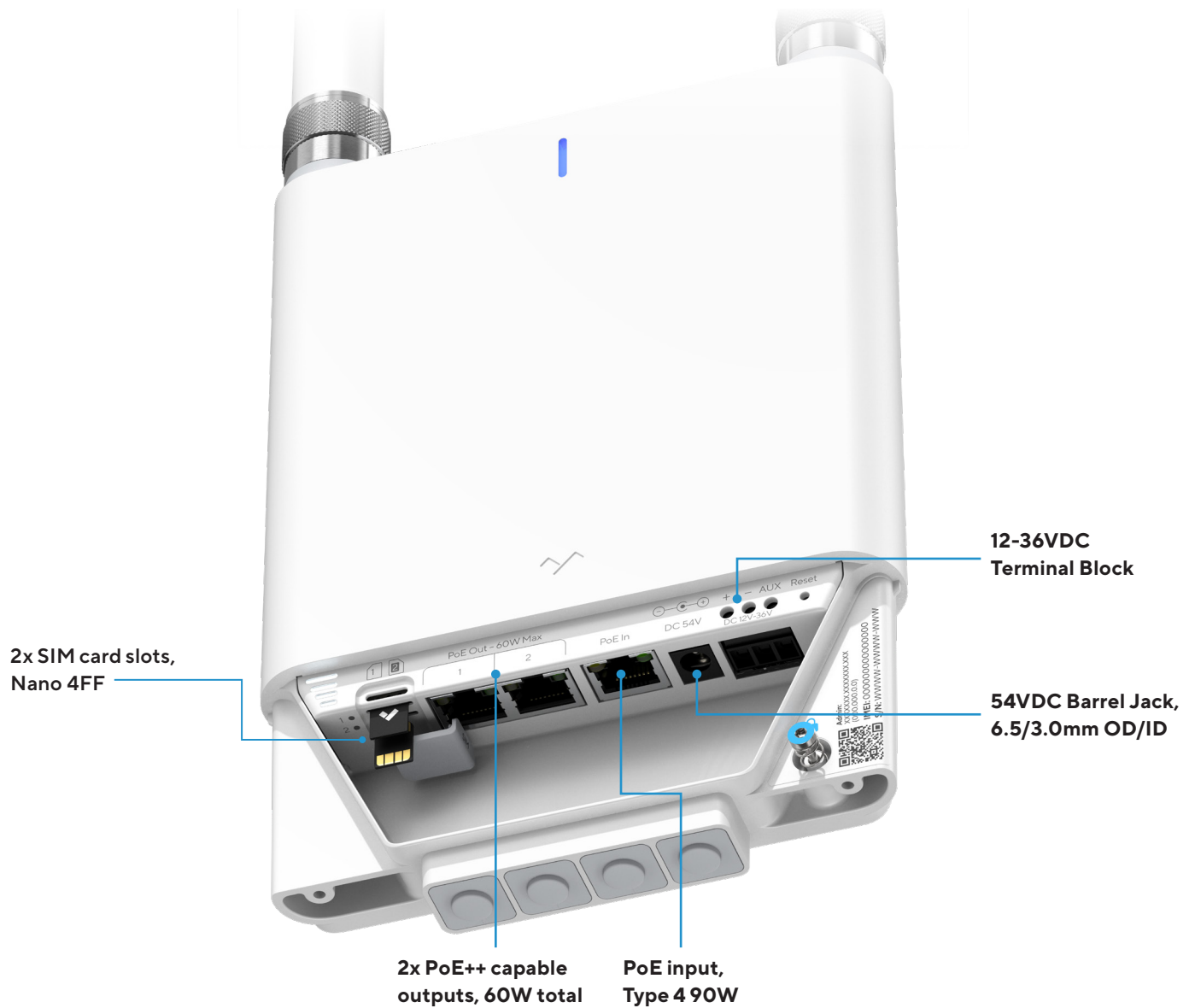
#### General

<b>Power Consumption</b>	9W above -25°C / -13°F 19W below -25°C / -13°F <b>Note:</b> Does not include connected devices	<b>Weight</b>	1.4kg / 3.0lbs
<b>Operating Temperature</b>	-40°C to 50°C / -40°F to 122°F	<b>LEDs</b>	1 status LED, 2 SIM indicator LEDs, 4 signal strength LEDs
<b>Humidity</b>	5-90% RH non-condensing	<b>Warranty</b>	10 years
<b>Dimensions</b>	Main Unit: L: 243mm / 9.6in W: 148mm / 5.9in H: 33mm / 1.3in Antenna: Ø: 25mm / 1.0in L: 179mm / 7.1in	<b>Included Accessories</b>	2 x N type antennas, mount plate, 2 x pole straps, 4 x wall anchors, 4 x wall screws, T10 security torx screwdriver, 4 x 7-9 mm cable grommets, 1 x 3-5mm cable grommet, 1 x 3-wire cable grommet
<b>Mounting Options</b>	Wall mount, pole mount, or mount on ACC-POE-90W-E		

1. Cellular carriers and operators throughout the world may only require telecom industry certifications such as PTCRB to operate on their network. Some carriers require additional testing and approval, beyond telecom certifications. A carrier listed in the approvals section means Verkada completed additional testing and acquired technical approval for that given carrier. Any carrier not listed may not require additional testing or approval beyond telecom industry certifications to operate on their network.



## GC31 Outdoor Cellular Gateway Inputs and Outputs





## Accessories

The GC31 Indoor Cellular Gateway comes with an AC/DC power adapter with a regionalized plug.

The GC31-E Outdoor Cellular Gateway has multiple power inputs and thus does not include power accessories. The following accessories are available from Verkada.



**ACC-POE-90W-E**  
Outdoor 90W PoE++ Injector

**Use case:**  
For powering the GC31-E in harsh environments. The GC31-E can be mounted directly on the injector.

[Datasheet](#)



**ACC-POE-90W**  
90W PoE++ Injector

**Use case:**  
For powering the GC31-E when the injector can be placed indoors or within a NEMA enclosure.

[Datasheet](#)



**ACC-ADAP-54V**  
AC/DC Power Adapter

**Use case:**  
Included with the GC31, but can be purchased for use with the GC31-E. Place the adapter indoors or within a NEMA enclosure.

[Datasheet](#)



**ACCX-TAP-DC100-E**  
AC/DC 7-Pin Light Pole Power Tap

**Use case:**  
Power the GC31-E by tapping into a streetlight. The power tap connects directly to AC and provides DC via PoE.

[Datasheet](#)



**ACC-ANT-10**  
Outdoor Directional LTE Antenna

**Use case:**  
Improves signal strength on the GC31-E when pointed toward the correct cell tower.

[Datasheet](#)

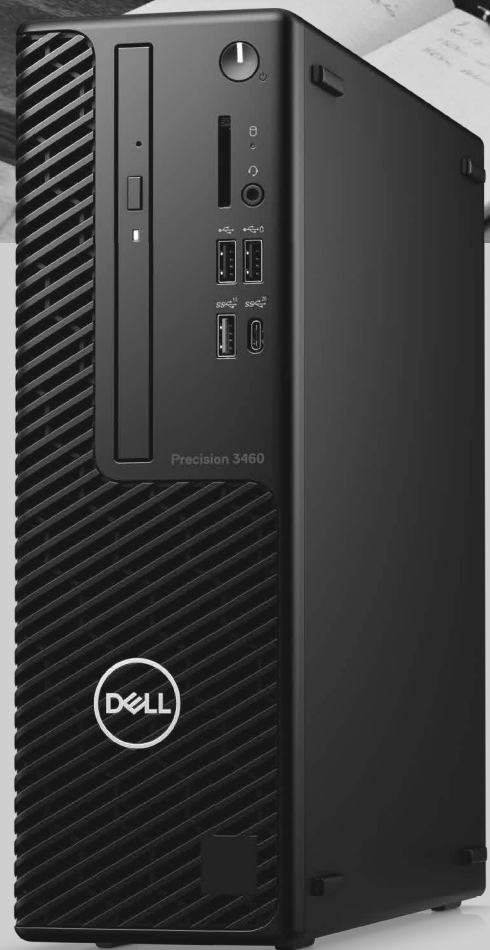
DELL Technologies

For use as operator control  
room workstations



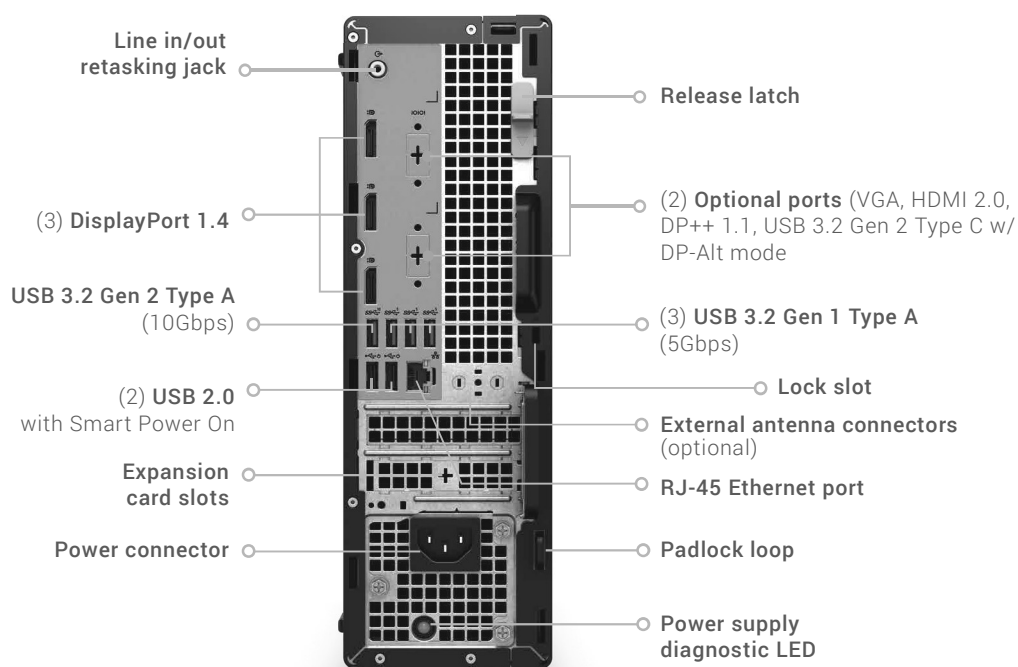
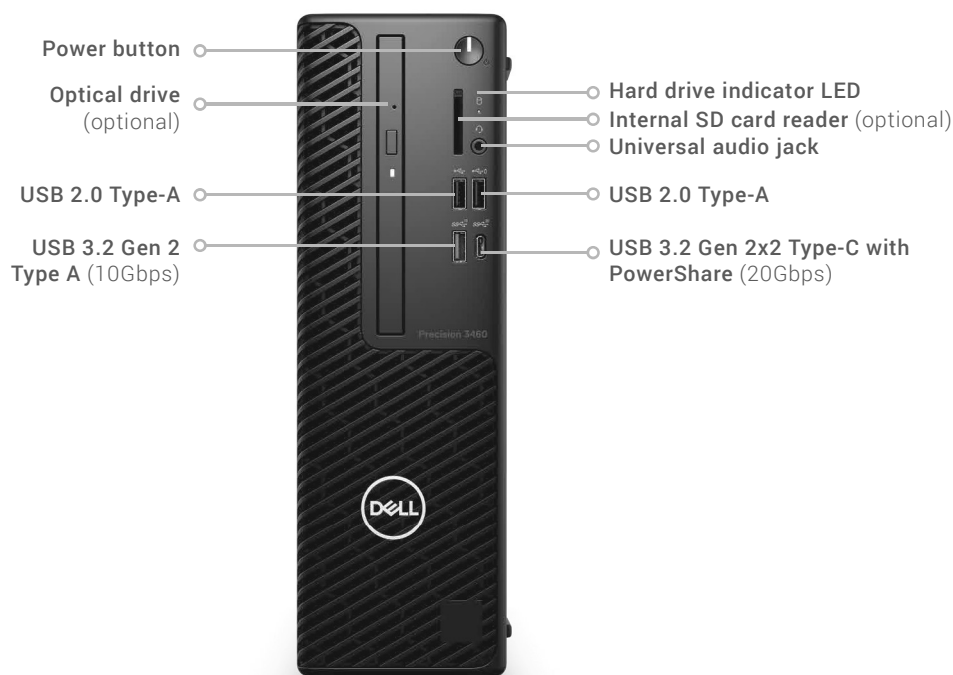
# Precision 3460 SFF

Smart performance  
and design



## Smart performance and design.

An intelligent, performance-optimized, space-saving small form factor workstation featuring AI-responsiveness.



► [Click here to review 360 degree product demo.](#)



# 2702L

## 27-inch LCD

Touchscreen Monitor



**Edge-to-edge design with  
integrated 10-touch**



**Optional Peripherals**



**Commercial-grade**

## Product Overview

The Elo 2702L 27-inch touchscreen monitor delivers a professional-grade interactive solution with Elo's industry-leading TouchPro® PCAP technology featuring edge-to-edge glass and enabling up to 10 simultaneous touches. The clear glass touchscreen provides exceptional image clarity, resolution, and light transmission for vivid images and details. Backed by a three-year warranty, the feature rich touchscreen monitor is equipped with dual built-in speakers and VGA and HDMI video connectors. With a compact form factor, clean design aesthetic and flexible mounting options, these touchscreens are well-suited for POS, interactive digital signage and self-service.

Designed for commercial use, the new Elo touchscreen monitor makes business operations easy delivering energy efficiency and versatile accessories. The 2702L accessories include MSR, barcode scanner, fingerprint reader, NFC, customer facing display and handles. Third party peripherals can be easily added as well with the integrated USB 2.0 hub.

**Create a seamless style across a variety  
of installations with interactive displays  
from 10 to 27-inches**

**Touchscreen is compatible with use of  
finger, glove and stylus**

**Multiple mounting options including -  
tabletop stand, wall mount and pole  
mount**



## 2702L 27-inch LCD Touchscreen Monitor

Specifications	
Color	Black
Diagonal Size	27" / 685.8 mm
Active Touch Area	23.54" x 13.24" / 597.88 mm x 336.31 mm
LCD Technology	Active matrix TFT LCD
Touch Technology	TouchPro PCAP
Number of Touches	10 Touches
Aspect Ratio	16:9
Native Resolution	1920 x 1080
Preset Video Timings	640 x 480 60Hz, 640 x 400 70Hz, 720 x 400 70Hz, 800 x 500 60Hz, 800 x 600 56, 60Hz, 1024 x 768 60Hz, 1280 x 720 @ 58Hz, 60Hz, 1280 x 800 60Hz, 1280 x 1024 60Hz, 1366 x 768 60Hz, 60Hz RB, 1440 x 900 60Hz, 60Hz RB, 1680 x 1050 60Hz, 60Hz RB, 1920 x 1080 50 60Hz
Number of Colors	16.7M
Brightness (typical)	Panel: 300 nits; with TouchPro PCAP: 270 nits
Response Time (Tr + Tf) (typical)	14 msec
Viewing Angle (typical)	Horizontal: 89°/89° or 178° total; Vertical: 89°/89° or 178° total
Contrast Ratio (typical)	1000:1
On-Screen Display (OSD)	Accessible through switches along the bottom. Controls: Menu, Power, Up, Down, Select Settings: Brightness, Contrast, Clock, Phase, H-position, V-position, Auto-Adjust, Aspect Ratio, Sharpness, Color Temperature, OSD Timeout, OSD Language, Volume, Mute, Recall Defaults, Audio Select, Power LED ON/OFF Languages: English, French, Italian, German, Spanish, Simplified Chinese, Traditional Chinese, Japanese, Russian, Korean Lockouts: OSD, Power
I/O Ports	VGA, HDMI, Combo Jack, DC Jack, USB Type B, USB 2.0 Type A, 4 x Micro USB
Peripheral Ports	4 x Micro USB side ports (Top, Bottom, Left, Right)
Video	VGA (VGA DE-15 (DB-15) Male connector cable included), HDMI (HDMI cable included) Input Video Horizontal Sync frequency range: 30 - 82KHz, Input Video Vertical Sync (frame rate) frequency range: 50 - 75Hz
Speakers	2 x 2W internal speakers
Power	Monitor input power connector: Coaxial power jack (2.1 mm pin outer diameter, 6.4mm barrel inner diameter); Monitor input power signal specifications: 12VDC +/- 5%; Adapter input voltage range: 100-240VAC, 50/60Hz; Power Consumption (Typical with monitor + AC/DC adapter): ON: 28W; SLEEP: 0.45W; OFF: 0.38W
Dimensions (H x W x D)	With Stand: 17.75" x 25.50" x 9.17" / 450.9 mm x 647.6 mm x 233 mm; Without Stand: 15.52" x 25.50" x 1.77" / 394.1 mm x 647.6 mm x 44.9 mm
Shipping Dimensions (H x W x D)	With Stand: 22.05" x 30.08" x 12.68" / 560 mm x 764 mm x 322 mm; Without Stand: 20.47" x 30.31" x 7.36" / 520 mm x 770 mm x 187 mm
Weight	With Stand: 23.15 lbs / 10.5 kg; Without Stand: 15.96 lbs / 7.24 kg
Shipping Weight	With Stand: 33.3 lbs / 15.1 kg; Without Stand: 21.12 lbs / 9.58 kg
Mounting Options	VESA 4-hole 100mm mounting interface on rear of unit
Temperature	Operating: 0° C to 40° C / 32°F to 104°F / Storage: -20° C to 60° C / -4°F to 140°F
Humidity (non-condensing)	Operating: 20% - 80% / Storage: 10% - 95%
Regulatory approvals and declarations	Canada CUL, IC; China CCC; Europe CE; United Kingdom UKCA; Korea KCC; Taiwan BSMI; United States FCC, UL; Japan VCCI; International CB; Australia RCM; Russia EAC; Mexico CoC; RoHS, China RoHS, WEEE, REACH
Ingress Protection	IPX 1 - Front only
Impact Protection	IK06
Warranty	3 years
Extended Warranty Option	4 year warranty coverage - Elo P/N: E898247 5 year warranty coverage - Elo P/N: E898449 3 year warranty coverage + AUR - Elo P/N: E898648 4 year warranty coverage + AUR - Elo P/N: E894921 5 year warranty coverage + AUR - Elo P/N: E895125
MTBF	50,000 hours demonstrated
Box Content	Touchmonitor, Quick Install Guide, 3 x Tie wraps, VGA cable, HDMI cable, Touch USB cable, Audio cable, Power brick, NA Power cable, EU Power cable, EEI Label, 4 x Screws (Only for E126483)

## Ordering Information

Part Number	Part Description	Mount	Technology	Surface Treatment	Touch Interface	Color
E351997	ET2702L-2UWA-0-BL-G	With Stand	TouchPro PCAP	Clear	USB	Black
E126483	ET2702L-2UWA-0-BL-NS-G	Without Stand	TouchPro PCAP	Clear	USB	Black

Learn more about Elo at [EloTouch.com](https://www.elotouch.com).

### Americas

Tel +1 408 597 8000  
elosales.na@elotouch.com

### Europe (EMEA)

Tel +32 16 930 136  
EMEA.Sales@elotouch.com

### Asia Pacific

Tel +86 (21) 3329 1385  
www.elotouch.com.cn

Elo reserves the right to change or update, without notice, any information contained herein; to change, without notice, the design, construction, materials, processing or specifications of any products; and to discontinue or limit production or distribution of any products. Elo, the Elo logo and TouchPro are either trademarks or registered trademarks of Elo Touch Solutions, Inc. All other trademarks are the property of their respective owners.  
© 2021 Elo Touch Solutions, Inc. All rights reserved. 21071AES00105



## DATASHEET

---

# AVEVA™ Edge

AVEVA Edge is a highly scalable, flexible software that provides the tools for everything from advanced HMI/SCADA applications to small-footprint embedded applications. The rich feature set enables users to create intuitive, secure, and highly maintainable HMI/SCADA applications for any industry.

### Choosing the right version of AVEVA Edge

- **AVEVA Edge SCADA** – The full Microsoft Windows-based runtime offers all the tools you need for advanced SCADA applications.
- **AVEVA Edge HMI** – AVEVA Edge for embedded systems such as Microsoft's Windows Embedded operating systems. The small footprint makes AVEVA Edge HMI ideal for embedded and edge machines.
- **AVEVA™ Edge IoT View** – AVEVA Edge IoT View is designed for Linux devices and enables edge computing on even small devices such as a Raspberry Pi.

AVEVA Edge offers an integrated development environment (IDE) that can be deployed to any runtime edition of AVEVA Edge.



## Enhancements in AVEVA Edge 2023

---

AVEVA Edge 2023 builds on previous enhancements and adds further capabilities and flexibility.

### IoT View enhancements:

- Dynamic Station ID (IP Address) for drivers {Curly Brackets}. Useful as Data Collection system and change PLC on the fly
- High Speed data logging improvements
- Support for new Linux Architectures and compilers (including 64 bit)

### Enhancements to the AVEVA Edge mobile access thin client:

- New custom keypad - HMI applications on a touch device need a virtual keyboard for input on operating systems without a native virtual keyboard
- Performance Improvements (In some cases more than 225% improvement)

### General enhancements:

- Modern User Interface/Icons (Align with other AVEVA HMI SCADA products)
- Add AVEVA Licensing support and new tag limits (1K, 2K, 10K, 100K, Unlimited tags)
- Ability to rename Classes (Structures) with propagation
- Support for AVEVA Industrial Graphics for SVG image import
- Built-In Functions to log to Azure IoT Hub and Worksheets

# AVEVA Edge features

(in alphabetical order)

**AVEVA Edge Management:** is a framework for provisioning software and managing remote devices at the edge.

Edge Management is a part of the AVEVA Connect, where AVEVA software can be provisioned easily, and users can access devices at the edge of the network to quickly update applications or monitor hardware remotely.

**Alarms:** Send online alarms or reports using multi-media formats like PDF. Alarms are real-time and historical. Log data in text file format or to any database. Use remote notifications to send alarms right to your inbox, printer or smartphone. Custom alarm fields allow you to customize up to ten additional fields to the alarm history.

**Animation:** Take command over graphics in a user-friendly interface. Paste images and even rotate dynamically using custom rotation points. Fill bar graphs with color or adjust the scale of objects with easy-to-use configuration. Other animations include command (for touch, keyboard and mouse interaction), hyperlink, text data link, color, resize, transparency/visibility and position.

**Business intelligence:** Log data directly to AVEVA™ Insight.<sup>2</sup>

**Cloud:** Natively connect with the cloud to take advantage of tools like AVEVA Insight or AVEVA™ Edge Management to get a holistic view of your business.<sup>2</sup> Pair edge devices running AVEVA Edge to the cloud and remotely monitor health and status or update applications.

**Database:** Connect to any SQL database (Microsoft SQL, MySQL, Sybase, Oracle), Microsoft Access, Excel, or ERP/MES systems (including SAP) – even from Microsoft Windows Embedded Compact Edition. The flexible built-in interface doesn't require knowledge of SQL. A patented solution allows for communication with SQL and relational databases running on any supported platform.

**Drivers:** Use over 100 native communication drivers for PLCs, temperature controllers, motion controllers, bar code/2D/Rfid readers, and many other devices. Use native drivers, connect to an OPC server, or use AVEVA driver toolkits to build your own drivers. Save time with comprehensive tag integration for PLCs. Drivers are included for Modbus, MQTT Sparkplug B, Allen Bradley, Siemens, Mitsubishi, Omron, Schneider-Electric and many others.

**Email:** Send emails (with attachments) or text messages that can be accessed from mobile devices. Get real-time information on alarms, process values and other events. Full runtime supports SSL encryption.

**Events:** Ensure traceability for operator-initiated actions or internal system activities. Log events such as security system changes (user logon or logoff), screen open/close, recipe/report operations, system warnings and any tag-value changes, including custom messages.

**FDA traceability:** Take advantage of built-in functionality to create 21 CFR part 11 compliant projects with traceability and e-signatures. These features are often used for pharmaceutical and food applications but can be used for any application where traceability is a requirement.

**FTP:** Automatically upload or download files during runtime to or from remote storage locations using the FTP protocol and flexible scripting functions. Configure FTP via scripting or the included interface.

**Graphics and design tools:** Create screens to meet any application requirement using the tools in the graphic interface. Combine over 1,000 animated objects to create any functionality required. Store graphics in the library for future use and easily give projects across an entire product line a consistent look and feel.

**Historian:** Load millions of values from SQL relational databases with optimized trend history, featuring data decimation. Easy-to-use tools provide quick access to statistical process control (SPC) values without any need for programming. AVEVA Edge offers add-on integration with AVEVA™ Historian (formerly Wonderware) and support for AVEVA Insight.<sup>2</sup>

**Import wizards:** Convert whole applications from FactoryTalk ME/SE, PanelMate or PanelBuilder 32. Save time when converting from a previously designed application to an AVEVA Edge application.

**IoT View:** AVEVA™ Edge IoT View is a platform-agnostic runtime for Linux and other embedded platforms. Make intelligent embedded systems and add your machines to the internet of things, industrial internet of things (IIoT), and Industry 4.0.

**Industrial graphics:** An additional graphics editor provides new tools and additional graphics and libraries. It includes extensive animations, situational awareness, style management and symbol import/export.

**Intellectual property protection:** Protect your intellectual property with just a few clicks of your mouse. Passwords protect individual screens, documents, scripts and worksheets. This prevents unauthorized viewing or editing of your project or application.

**JavaScript custom widgets:** Custom widgets expand and enhance the graphical interface by integrating third-party, reusable JavaScript, HTML5 and CSS interfaces, properties and events. Use included custom widgets such as pie chart, tree view, calendar, image list and web browser – or create your own.

**Mobile access:** This thin client allows you to access your graphical interface from any device, with a browser that supports HTML5 devices, such as iPads, iPhones, Android devices, Windows devices and others. AVEVA Edge now includes support for all native objects and allows you to integrate third-party web-based controls.

**Multi-language:** Develop your application in one of many development languages, including English, Portuguese, German, French, Polish, Russian, Chinese (traditional and simplified), Japanese and Spanish. Or use external translation tools to switch the runtime to any language. AVEVA Edge offers automatic font replacement based on the language selected.



**Multi-touch interface:** Develop applications for touchscreen devices. AVEVA™ InTouch Edge HMI's multi-touch interface allows development for any touchscreen-enabled device. Use familiar, modern interface gestures, like pinch zooming and panning. Use swiping gestures to scroll through alarms, change screens or execute other commands. Inertia in the multi-touch interface offers a comfortable user experience. Rotate graphics, dock screens and take advantage of features like dual-touch command.

**.NET and ActiveX:** Use third-party controls to enhance your project. AVEVA Edge is a container for .NET and ActiveX controls, allowing you to add functionality such as browsers, media players, charting, live streaming from cameras, and other ActiveX or .NET controls.

**OEM:** AVEVA Edge can be customized for OEMs who want to offer pre-installed HMI or SCADA software on their hardware, or for OEMs who want to add value to their machines by offering remote monitoring, maintenance or customizable applications.

**OPC:** AVEVA Edge provides native OPC interfaces, such as OPC UA (client/server), OPC DA (client/server), OPC XML (client), and OPC HDA (server). OPC UA and OPC DA also offer native redundancy configuration and tag integration for OPC DA and OPC UA servers.

**PDF export:** Send alarms, reports, text files or Microsoft Word documents in portable document format (PDF) to a production supervisor, quality manager or maintenance worker using the included PDF writer.

**Recipes:** Save time and maintain consistency by automating part parameters or production quantities with flexible recipe management tools. Options include loading directly to PLC or editing before committing to PLC.

**Redundancy:** For critical applications where data is vital, AVEVA Edge supports web server, database and overall system redundancy to protect your information.

**Reports:** Create clear, concise reports in plain text, RTF, XML, PDF, HTML, and CSV – or integrate with Microsoft Office programs such as Excel. Get the data you need, in the format you need it, to make informed decisions. AVEVA™ Reports for Operations also offers advanced operational reporting for AVEVA Edge.<sup>2</sup>

**Scalable:** Use the same development environment to design and deploy projects to a wide range of platforms, such as Linux, Windows Embedded, Windows CE, Windows 8.1, Windows 10, Windows 11, Server 2012 R2, Server 2016, Server 2019, and Server 2020 editions.

**Scheduler:** Schedule application behavior triggered by tag changes, date/time, frequency, or any other trigger. Trigger reports at a particular time of day – or even trigger driver worksheets to read/write at a scan rate you choose, or use the scheduler for simulation.

**Scripting:** AVEVA Edge supports several powerful scripting languages, built-in AVEVA Edge functions and standard VBScript. Take advantage of widely available resources for VBScript. Both the native AVEVA scripting language and VBScript can be used simultaneously to give you the functionality you need, even from thin clients. Script debugging tools for the native VBScript editor include breakpoints and a variable watch list to improve scripting productivity. Included with industrial graphics is the flexible and powerful Quick-Script language.

**Security:** AVEVA Edge includes support for group and user accounts, e-signatures and traceability. You can integrate your project to the Active Directory (users and groups).

**Symbols:** The included native graphics library features push buttons, pilot lights, tanks, sliders, meters, motors, pipes, valves and other common objects. Use the 1,000+ included symbols in your project, modify existing symbols to suit your needs, or create your own from scratch. AVEVA Edge supports third-party symbol libraries and graphic tools. Industrial graphics add additional symbol libraries, including situational awareness graphics that make it easy to understand what is happening.

**Standards:** Use common standards to develop applications that are compatible with TCP/IP, .NET, ActiveX, OPC (client and server), ADO/ODBC, COM/DCOM, OLE, DDE, XML, SOAP, REST and HTML5.

**Tag database:** AVEVA Edge features an object-oriented database with boolean, integer, real, strings, arrays, classes (UDT/structures), indirect tags and included system tags. Built-in functions allow you to create, delete or modify the tags database settings during the runtime. With this feature, you can design generic templates that can be easily customized to each project, even during the runtime. AVEVA Edge also offers tag integration from a wide range of PLCs, including Schneider Electric.

**Templates:** AVEVA Edge has many templates and sample applications available including: andon, digital OEE, PackML and business intelligence.

**Trends:** AVEVA Edge supports real-time and historical trends, as well as SPC functionality. Log data in binary format to any local or remote SQL database, or to AVEVA Historian (formerly Wonderware) or AVEVA Insight. Color or fill trends with graphic elements to enhance clarity of data. Date/time-based or numeric (X/Y plot) trends give you the flexibility to display information that best suits your application. AVEVA Edge supports vertical and horizontal trending.

**Troubleshooting:** Quickly debug and verify a project using local and remote tools for troubleshooting, including status fields, HTML5-based DatabaseSpy for AVEVA Edge IoT View, Watch Window, and LogWin. Capture screen-open and close times, see communications in real time, messages related to OPC, recipes/reports, security, database errors and even custom messages. Finish your project quickly using these powerful tools.

**XML screen toolkit:** Modify or create screens during the runtime or import screens that you've created.<sup>2</sup>



## Overview

AVEVA Edge is a comprehensive platform that includes all the tools you need to make SCADA and HMI applications that have real power behind them. The environment allows you to develop once and deploy anywhere.

AVEVA Edge also offers a runtime edition (AVEVA Edge IoT View) available for Linux.

## References

<sup>1</sup>See Microsoft KB5004442 – Manage changes for Windows DCOM server security feature bypass (CVE-2021-26414)

<sup>2</sup>Additional purchase required

For more information about AVEVA Edge, visit:  
[aveva.com/en/products/edge](https://aveva.com/en/products/edge)

**AVEVA**

aveva.com

© 2023 AVEVA Group Limited and its subsidiaries. All rights reserved.  
 AVEVA and the AVEVA logo are a trademark or registered trademark of AVEVA Group Limited in the U.S. and other countries.  
 All product names mentioned are the trademarks of their respective holders.

## NX1 Machine Automation Controller

Continue to pursue productivity



The image shows a hand holding an Omron NX1 Machine Automation Controller. The controller is a black and silver unit with multiple ports and status indicators. The text on the controller includes "NX102-1200", "OMRON NX1", "PORT1 EtherNet/IP", "PORT2 EtherNet/IP", "PORT3 EtherCAT", "RUN", "ERROR", "BUSY", "PWR", "BUSY", "NET RUN", "NET ERR", "L/A", "POWER", "A", "B", "1", "2", "3", "4", "5", "6", "7", "8", "A", "B", "SW", "SET".

The solution in your hand

Secure data transfer | Machine control | Safety integration | Traceability | Quality inspection



# Improve productivity, improve your business

The manufacturing industry is under pressure to keep boosting productivity without compromising on quality. Global production and flexible production are required to satisfy diverse consumer needs.

In addition, manufacturers need to control quality and enhance safety to meet advanced regulatory requirements. In order to fulfill these requirements, it is crucial to utilize information, take safety measures, control quality, and at the same time improve production efficiency.

## Common issues

### Customers compromise between production efficiency and information utilization/safety measures/quality control



#### **Production cycle time is increased due to data traceability requirements**

Full traceability is required to meet high-level quality standards.



#### **Safety measures make setup and troubleshooting difficult**

Separate safety control for machines and lines and separate controllers for machine control and safety are required. Line and machine design is time-consuming, and safety measures have to be redesigned when the layout is changed.



#### **Production lead time is increased due to additional inspections and tight quality control**

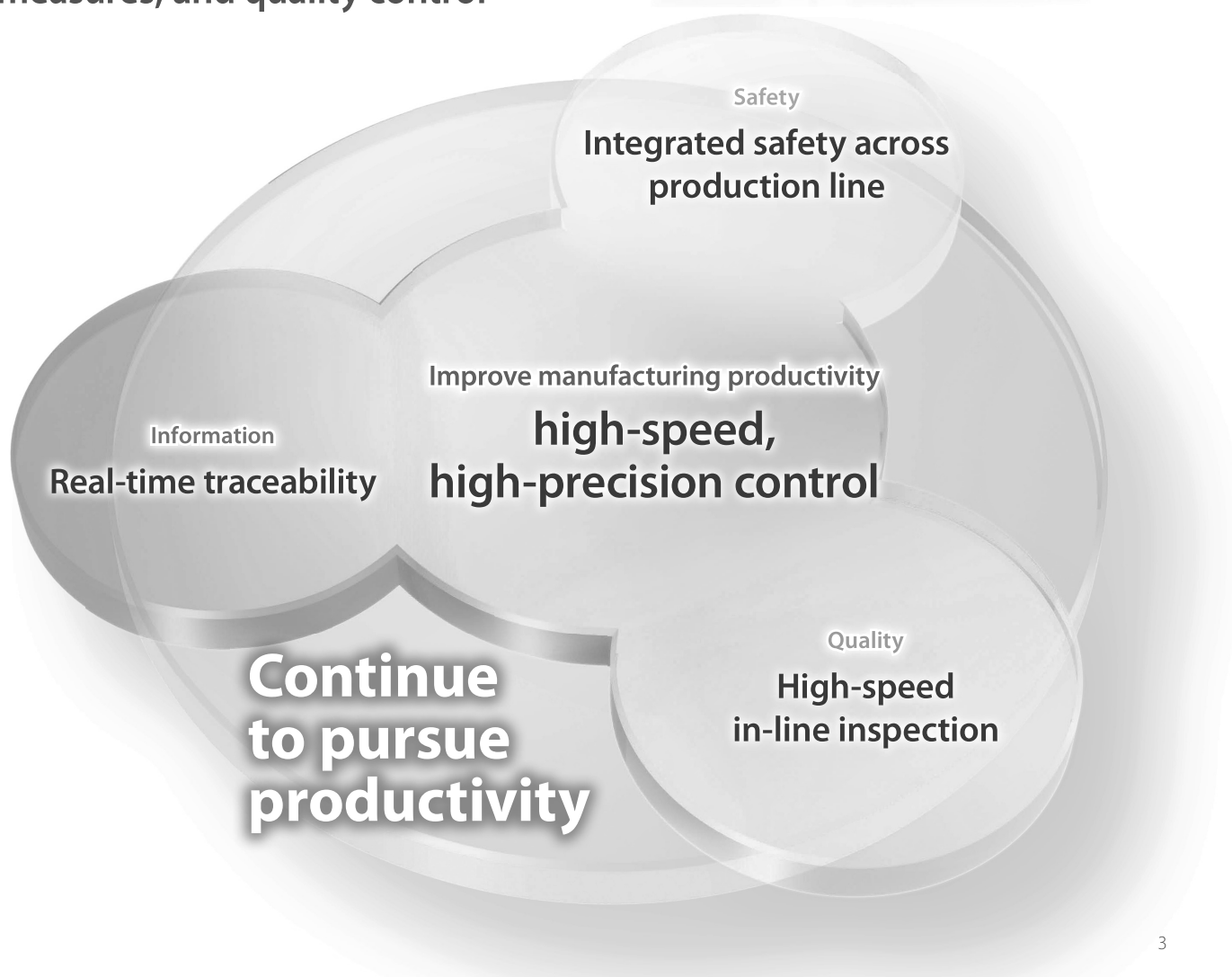
Adding inspections to maintain quality increases production lead time. When special machines with built-in PC that collect and process data at high speeds are used for inspections, maintenance becomes difficult. Instead, acceptance sampling is conducted offline.

# NX1

The next standard

## NX1

Improves production efficiency while optimizing information utilization, safety measures, and quality control



# Produce faster without compromising on quality

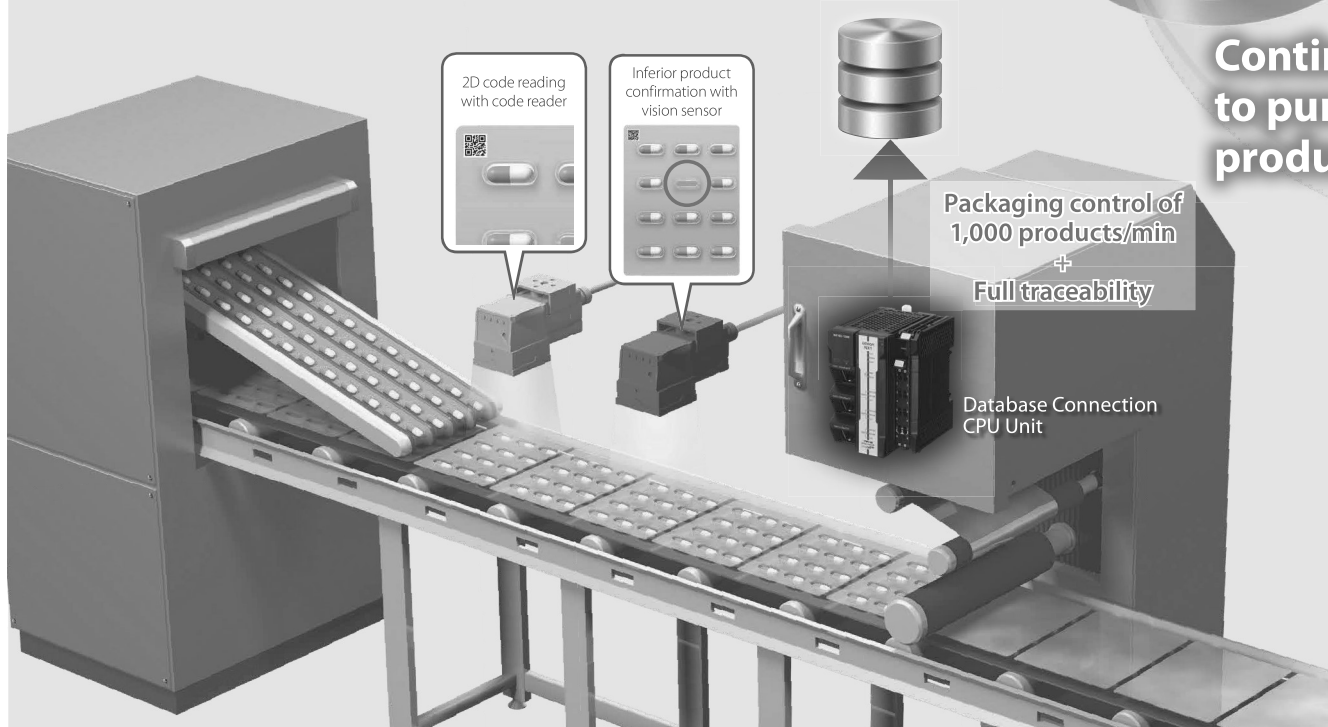
The NX1 can securely transfer information, take safety measures, and control quality while at the same time improving production efficiency through high-speed, high-precision control.

This contributes to continuous improvement in productivity.

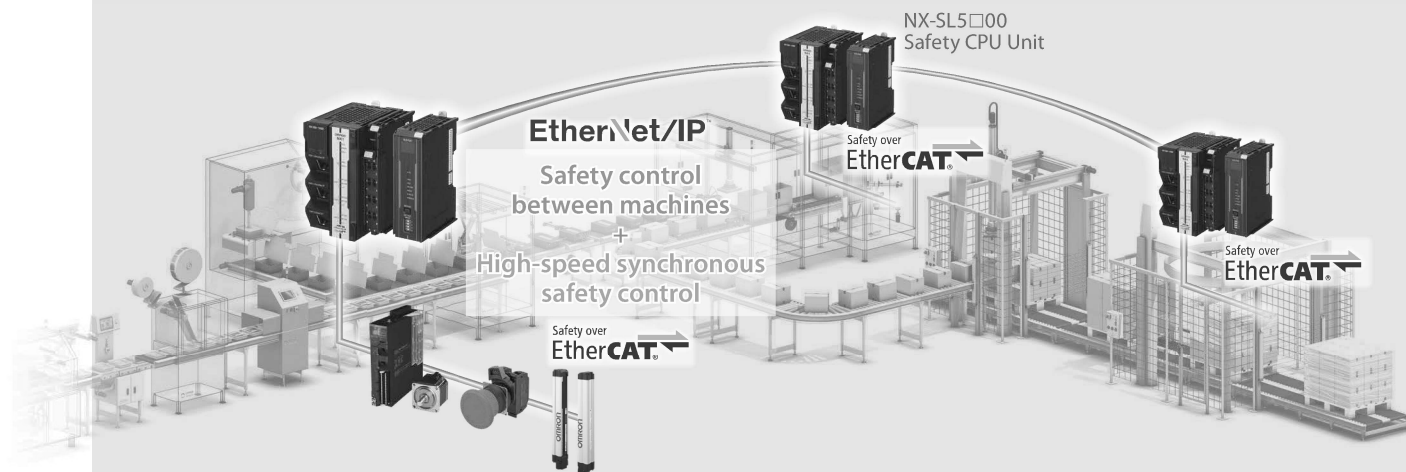


## Real-time traceability

The NX1 provides high-speed control while utilizing information. For example, the NX1 used for a packaging machine with the capability of handling 1,000 products per minute can collect all traceability data in synchronization with the production cycle while performing motion control.



# Integrated safety across production line



The NX1 is the first in the world\* to integrate two different open networks: EtherNet/IP™ for scalable safety control in production lines and EtherCAT® for fast, reliable, redundant safety control in machines. Furthermore, it integrates safety control into machine control in lines that require fast cycle times.

This integration allows you to standardize machines and build flexible lines.

\* Based on Omron investigation in March 2018.

Safety

Improve  
manufacturing  
productivity

Quality

## High-speed in-line inspection

Although special inspection machines with built-in PC are widely used for high-speed inspections, they require special maintenance skills.

Therefore, acceptance sampling is often carried out offline to prevent line stoppages. The NX1 can be used in conjunction with the High-speed Analog Input Unit to collect measurement data within a fixed cycle time of 5  $\mu$ s. This standard controller eliminates the need for special machines with PC and can be maintained by on-site engineers. In-line inspections of all products can also be conducted easily.

High-speed in-line  
inspection of all products  
with standard inspection  
machine



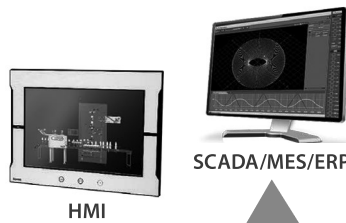
NX-HAD@@@  
High-speed Analog  
Input Unit

# Seamless integration: production line & IT systems

The NX1 Controller integrates inputs, logic, outputs, safety, and robotics, offering a wide variety of applications that leverage information to boost productivity and measures for quality and safety.

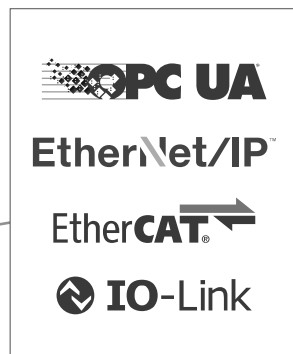


**Secure direct  
connection to database**



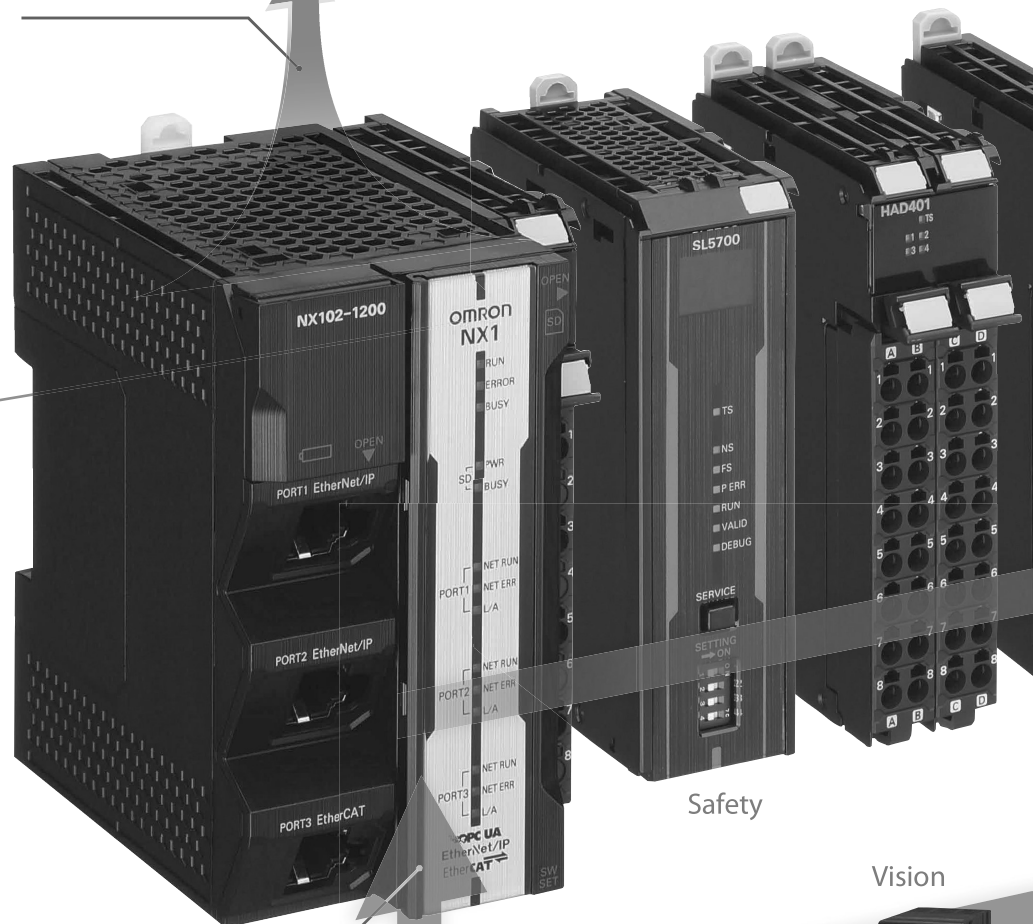
- Microsoft SQL server
- Oracle Database
- IBM DB2
- PostgreSQL
- MySQL
- Firebird

**Networks**



**High-speed, high-precision control:  
Synchronized within same cycle**

The NX1 provides synchronized control of the NX bus connected I/O and motion control network within same system cycle time and jitter below 1  $\mu$ s. This enables real-time data collection and analysis as well as high-speed, high-precision control.



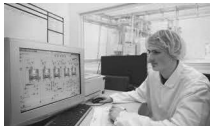
**Safety**

**Vision**


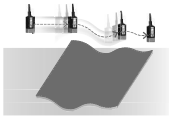
**Motion**




Information  
utilization  
application

Application	NX1 functionality + product
<b>All traceability data storage</b> 	NX1 Database Connection CPU Unit Code reader RFID
<b>Direct connection of machine to MES/SCADA</b> <b>Data utilization to prevent manipulation</b>	NX1 OPC UA server (standard functionality)
<b>Linkage between image and data</b>	FH Vision System

Production  
efficiency  
improvement  
application

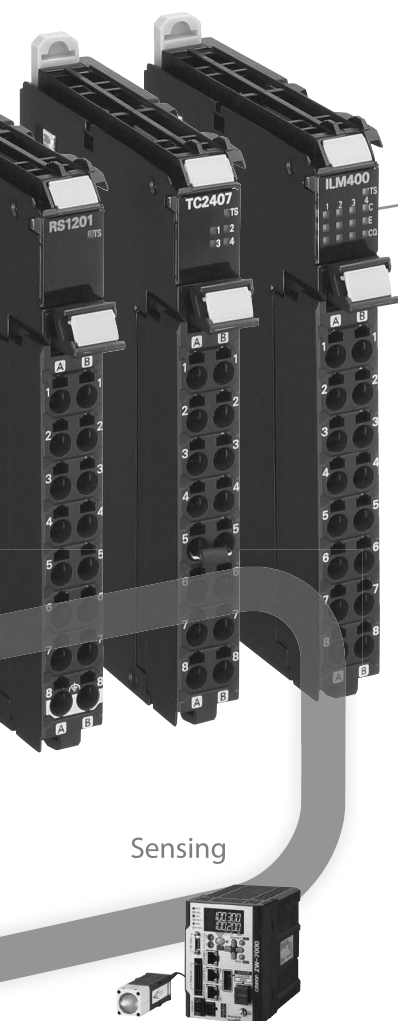
Application	NX1 + product
<b>Predictive maintenance</b>	<b>NX-ILM400</b> IO-Link Master Unit IO-Link sensor
<b>Automatically optimized temperature control</b> 	<b>NX-TC@@@</b> Temperature Control Unit E5@D Digital Temperature Controller
<b>Position and load control for servo press</b>	1S Servo System
<b>Weighing control</b>	<b>NX-RS@@@</b> Load Cell Input Unit
<b>Tracer control</b> 	ZW-7000/5000 Confocal Fiber Displacement Sensor

Quality control  
application

<b>Rotator inspection</b>	<b>NX-HAD@@@</b> High-speed Analog Input Unit
<b>Welding quality inspection</b>	
<b>Appearance inspection</b> 	FH Vision System

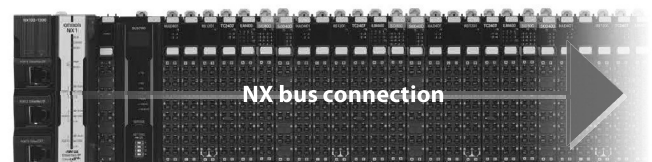
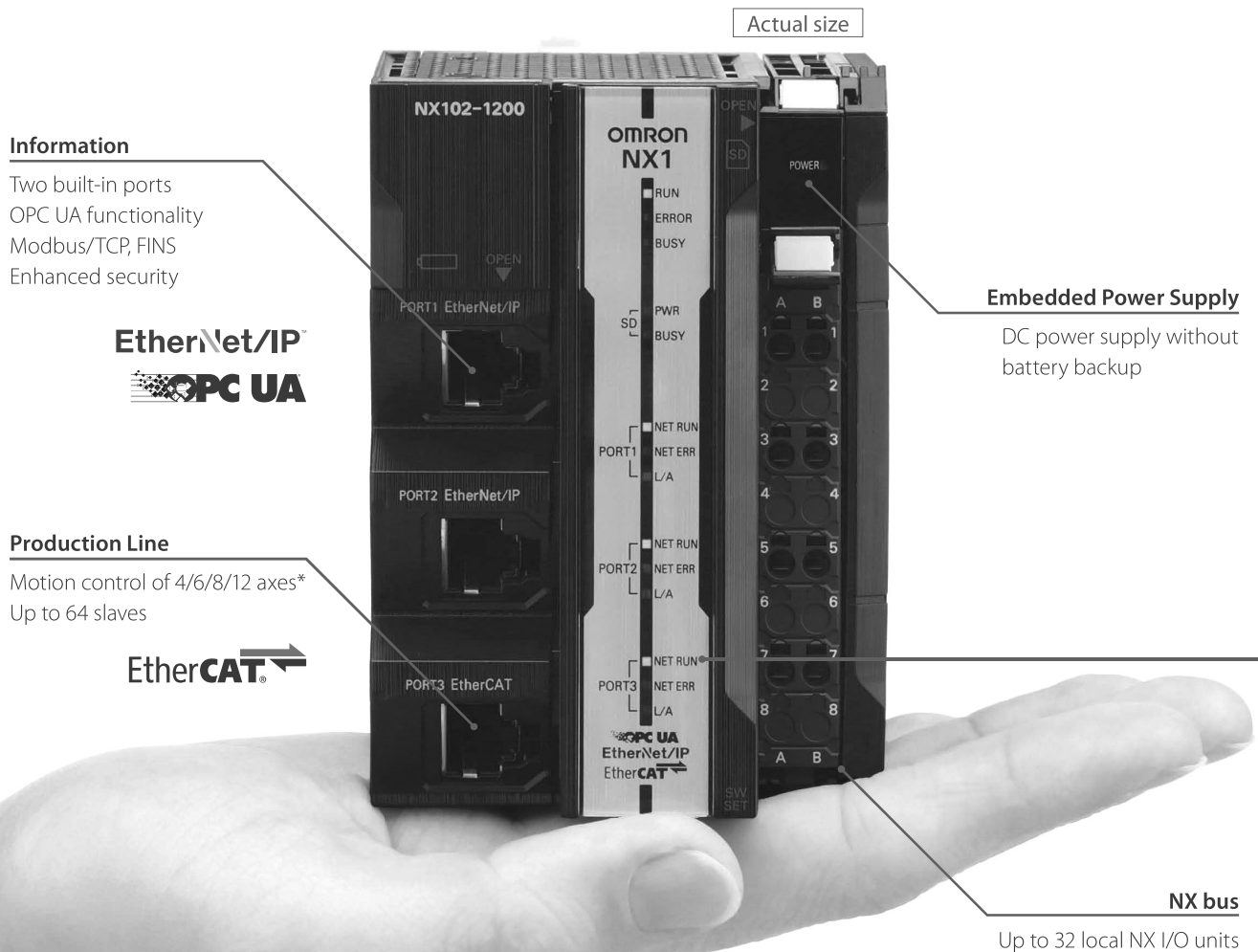
Safety measures  
application

<b>High-speed safety control in machine</b>	<b>NX-SL5@00</b> Safety CPU Unit
<b>Safety control in line</b>	
<b>Intrusion detection</b> 	F3SG-R Safety Light Curtain



# NX1 brings advanced control in miniaturized size

Three industrial Ethernet ports and a power supply are housed in a compact design with a width of 66 mm. The NX1 provides key functionality to integrate control and information for advanced manufacturing applications. The new controller contributes to the pursuit of productivity improvements.



## High-speed, high-precision control

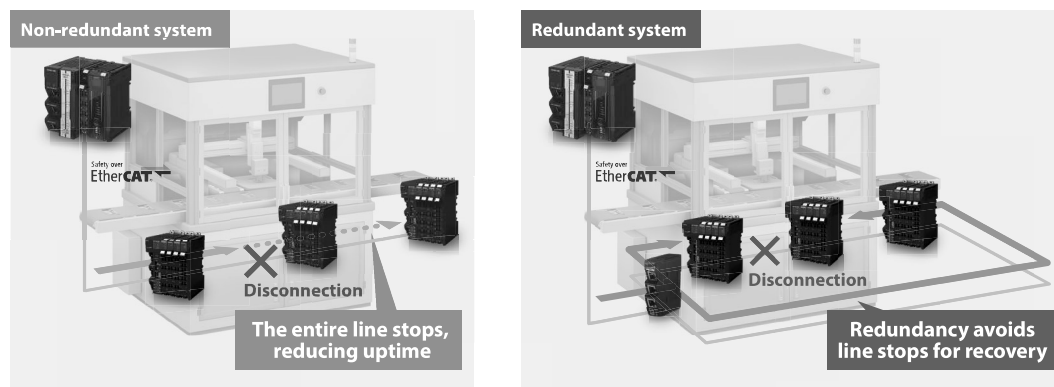
Synchronized control of I/O and motion within 1 ms cycle time

Jitter : 1  $\mu$ s

Memory capacity for variables : 33.5 MB<sup>\*1</sup>

## Redundancy to minimize downtime (NX102-□□00)

Even if a part of the EtherCAT network is disconnected, Cable Redundancy provides continuous connectivity. This function allows you to fix disconnection without stopping the machines and production line where one controller provides both machine control and safety control.



## Multicore microprocessor for control and data handling

The multicore microprocessor enables information utilization including communications and traceability without compromising control performance.

## Secure host connection

OPC UA is an IEC communication protocol which is listed as a recommendation for Industrie 4.0 and PackML. The NX1 comes equipped with an OPC UA server interface and provides a secure connection to IT systems such as MES and ERP.



## Enhanced Ethernet functionality

Connectivity to existing devices (e.g., Modbus/TCP<sup>\*2</sup>, FINS communications, and connection to other vendor PLC<sup>\*3</sup>) and EtherNet/IP<sup>™</sup> performance (increased to 12,000 pps<sup>\*4</sup>) are improved. Packet Filter enhances security, and visualization of EtherCAT<sup>®</sup> slave errors makes troubleshooting easier.

<sup>\*1</sup>. The total number of bytes of retained and non-retained variables.

<sup>\*2</sup>. Clients instructions are supported.

<sup>\*3</sup>. SLMP commands are included in the Sysmac Library.

<sup>\*4</sup>. The total pps of two ports.



# One software for easy integration & simulation

Sysmac Studio – Integrated Development Environment integrates programming, configuration, information, and safety.

The project version control system in the Sysmac Studio Team

Development Option ensures smooth development across the team.

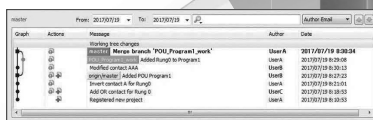
The Sysmac Studio includes Function Blocks for motion control and

database connection, and collections of software functional components Sysmac Libraries can be downloaded from our website. These allow you to minimize time to build systems that boost productivity.

Sysmac Studio



- Fully conforms with IEC 61131-3 standards
- PLCopen Function Blocks for Motion Control



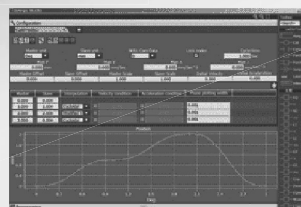
Project version control function



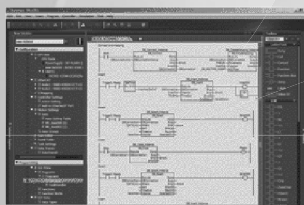
Safety



Safety Function Blocks



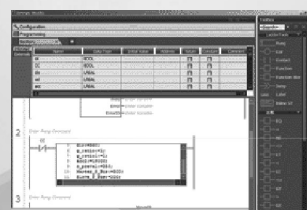
Motion control



Information utilization



DB connection Function Blocks



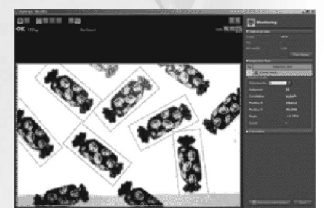
Programming



HMI



Motion Function Blocks



Vision



High-speed Analog Inspection Library



# MicroComm DXL

## DXL System Data Sheet

### Description

The MicroComm DXL digital intercom system is designed to be cost effective for applications with widely distributed architectures and those of a smaller scale. It is also ideally suited for adding functionality and flexibility when retrofitting relay switched intercom systems. A comprehensive feature set gives the MicroComm DXL the power to handle projects with the most demanding requirements, and like all MicroComm family members, it incorporates digital audio technology and provides a high performance, rugged, and reliable communication solution.

Two basic building blocks form the backbone of the system. Digital Communication Controllers (DCC) are the master component of each exchange and can be interconnected to form larger systems. They incorporate the exchange processor, control software, configuration data, and network ports as well as the intercom station, master station, and audio interface boards. Digital Communication Expanders (DCE) and Talk Back Expanders (TBE) are used to increase the capacity of each exchange. Up to four DCE and/or TBE expander units can be connected to each DCC controller.

The MicroComm DXL is compatible with the same set of intercom stations, master stations, and call devices as the rest of the MicroComm family. The wide and growing variety of standard stations and specialty stations is therefore available for your use, regardless of which MicroComm system you choose.

A key feature of the MicroComm DXL is the DXL Administrator Software. This Windows Explorer style user interface runs on a standard PC and provides system configuration, logging, and diagnostic functions. With its easy to follow tree structure, simple to understand data entry dialogs, copy and paste device creation feature, and built-in device libraries, a MicroComm DXL is easy and quick to program.

### FEATURES

#### System Architecture

- Simple, modular system architecture
- Digital audio trunks and signal processing
- Each exchange can function independently
- Exchanges can be networked to form large systems
- Unrestricted communications within each exchange
- Twenty-six channel audio trunk interconnects exchanges
- Supports MicroComm family master stations
- Full touch screen and graphic panel master control
- Telephone sets provide administrative master functions
- Supports MicroComm family intercom stations
- Supports generic 25 volt intercom stations
- Supports MicroComm Discrete Input/Output modules
- 64 x 128 pixel graphics display



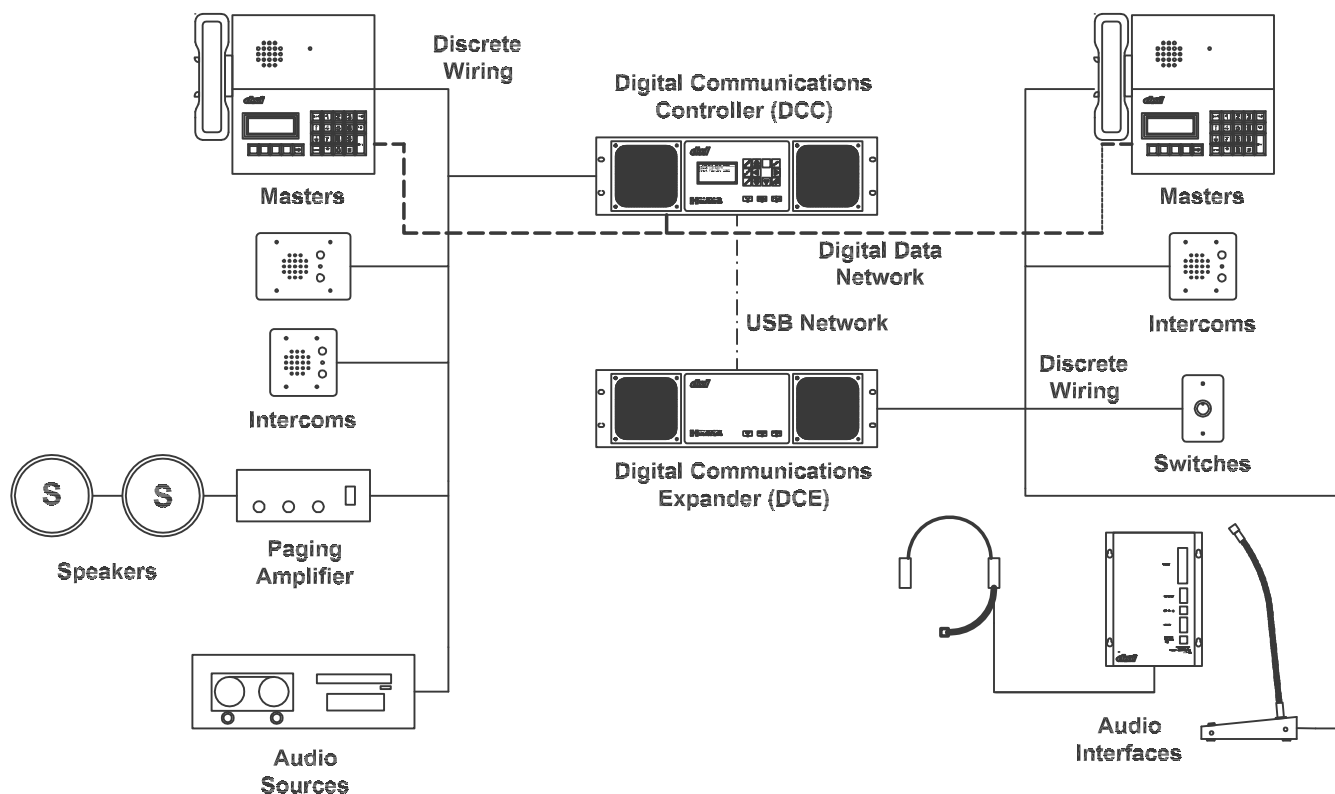
- Eleven button keypad with menu driven interface
- Built-in monitoring and self-test routines

#### Operating Features

- Paging and program distribution to audio outputs and stations
- Audio Level Alarm threshold detection
- Sequential and group audio listen-in monitoring
- Hands free and press-to-talk operator control
- Multiple priority levels for each category
- Individual audio control for each channel
- Master groups for parallel operator control
- Six program distribution channels in each exchange
- Six system wide program distribution channels
- Flexible operational tone signaling
- Time clock and event controlled tone signaling
- Tones and messages recorded as WAV audio files
- Master station and visiting booth call recording
- Unit unmanned and time out call forwarding
- Call and program switch enabling/disabling
- Flexible display master menu architecture
- CCTV switcher and visiting booth support

#### DXL Administrator Software Features

- Windows Explorer style configuration



## DXL Exchange

- Operates on standard PC or laptop computer
- Loads and validates configuration files
- Functions both on-line and off-line
- Provides configuration, logging, and diagnostics
- Devices displayed in both tabular and window formats
- Device library included for standard devices
- Add new devices with copy and paste commands
- Remote system access available via modem
- Manages the entire system through a single port
- Manages system security features

Identification Numbers (up to 5 digits) 99999

DCC/DCE Capacity  
 Intercom Stations (half duplex) 32  
 Master Stations 2  
 Audio line inputs 2  
 Audio line outputs 2

Exchange Capacity  
 Intercom Stations (half duplex) 160  
 Master Stations 10  
 Audio line inputs 10  
 Audio line outputs 10

System Capacity  
 Exchanges 32  
 Intercom Stations (half duplex) 5120  
 Audio Line Inputs 320  
 Audio Line Outputs 320

## Specifications

### General

Audio band width 300-3,500 Hz  
 Audio Signal Processing Digital  
 Audio Switching System Digital Time Space Switching  
 Control Network Ethernet and USB  
 I/O Network LonWorks





# MicroComm DXL

## DCC Digital Communication Controller

### Description

Digital Communication Controllers (DCC) are the heart of the MicroComm DXL system. Each DCC contains all processing, control software and configuration data to operate independently as a stand alone exchange. Exchange networking, host port control, programming, diagnostics, and maintenance are all performed through the DCCs.

Each DCC also supports two intercom or telephone master stations and 32 intercom stations\*. Two line-level audio inputs and two line-level audio outputs with control and status allow connection of microphones, program sources, paging amplifiers, and logging recorders. The front panel keypad and display are used for basic system set up and diagnostics.

Up to 80 exchanges can be interconnected to form large systems.

### Features

- 2 master stations per DCC
- 32 intercom stations per DCC
- 4 DCEs and/or Talk Back Expanders per DCC
- Simple, modular system architecture
- Digital audio trunks and signal processing
- Each exchange can function independently
- Exchanges can be networked to form large systems
- Unrestricted communications within each exchange
- Twenty-six channel audio trunk interconnects exchanges
- Supports MicroComm family master stations and telephone sets (POTS equivalent) used to perform administrative master functions
- Supports MicroComm family intercom stations as well as 25 volt generic stations
- Full touch screen and graphic panel master control
- Supports MicroComm Discrete Input/Output modules
- 64 x 128 pixel graphics display
- Eleven button keypad with menu driven interface
- Optional audio level alarm detection support
- Built-in monitoring and self-test routines
- Automatically senses type of power supply voltage

### Specifications

Physical Form Factor	3 U rack mount 5.22" x 19" x 16.13" (13.3 x 48.3 x 41.0 mm)
Environmental	
Operating Temperature	32 to 122 °F (0 to 50 °C)
Storage Temperature	-40 to 158 °F (-40 to 70 °C)
Humidity	0 to 95 % non-condensing
Power Requirements	100 - 120 Vac, 60 Hz, 2.75 A max (Power supply is rated at 6 A max)



#### Field Connections

Input power	AC line cord
Master stations	DB-15
Intercom stations	DB-37
Intercom station switches	DB-25 (with 300 series stations)
Audio inputs/outputs	RCA phono jack
Status inputs/outputs	Screw terminals
Modem	RJ-11
Ethernet	RJ-45
Audio Trunk	DB-9 or Fiber Optic
USB	2 type A
Serial outputs	2 DB-9

#### Line Outputs

Output 1.77Vrms (max) into a  
600 ohm (min) load

#### Line Inputs

Impedance > 10K

#### Cabling

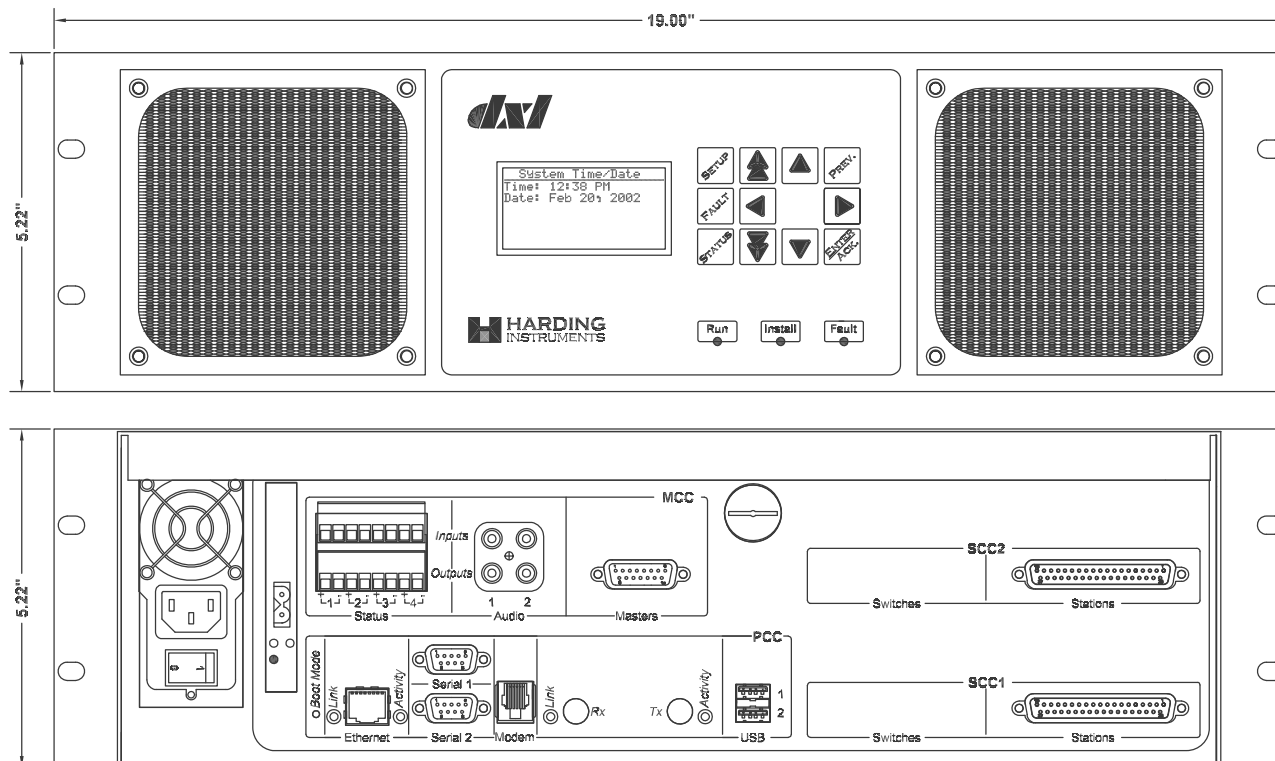
Audio	22 ga shielded twisted pair max 2500 ft (750 m)*
Switches	(Generic 300 series stations only) 22 ga unshielded twisted pair max 2500 ft (750 m)*
Fiber (Audio Trunk)	2 fibers - 62.5/125 $\mu$ m multimode ST connectors, 10 dB power budget, 820 nm wavelength

#### Standards

FCC Part 15, UL, CSA

\*Wiring from an exchange to the outside of a building requires adequate lightning protection.

## Mechanical



## Ordering Information

DCC-XXAA-BBCC-DDEE-FFGG

Option	XX	AA	BB	CC	DD	EE	FF	GG
Series Identifier	XX	AA	BB	CC	DD	EE	FF	GG
Security	S1							
Master Control Card								
None		00						
2 Intercom Masters		M4						
2 Telephone Masters		T4						
Combination 1 Intercom and 1 Telephone		C4						
SCC1 Cards								
None			00					
SCC-300 Card			30					
SCC-400 Card			40					
SCC-401 Card			41					
SCC2 Cards								
None				00				
SCC-300 Card				30				
SCC-400 Card				40				
SCC-401 Card				41				
Process Control Card								
Standard PCC					S1			
Enhanced PCC (includes ALA)					E1			
Audio Trunk Option								
None						00		
Copper Audio Trunk						CU		
Fiber Optic Audio Trunk						FO		
Internal Modem								
Internal Modem							MD	
PCI Card Slot Device								
None								00
LonWorks Card								LW
VoIP Card								IP

Document # DS-DXL-DCC-1.22 • Copyright © 2004 Harding Instrument Co. Ltd. • All Specifications subject to change without notice • Printed in Canada



9564 Yellowhead Trail NW  
Edmonton, AB T5G 0W4  
sales@harding.ca

Tel 780.462.7100  
Fax 780.450.8396  
www.harding.ca



Represented by:



## QCB-120-(1-4) Quick Connect Board

### Description

The QCB-120 Quick Connect Board is used with MicroComm DXI and DXL intercom systems, to simplify the field wiring when connecting stations to an exchange. The QCB-120 has a terminal block, arranged in tiers, and a female DB connector. The QCB-120 is used with an interface cable, which has two male DB connectors (one on each end). One end plugs into the station audio board and the other the QCB-120. The field wiring from each station connects to screw clamp terminals, one on each tier. Terminal blocks on the QCB-120 are supplied with three tiers for shielded pairs (audio lines), two tiers for unshielded pairs (switch connections) for one unsupervised input switch, and three tiers for two unshielded pairs for two supervised input switches.

QCB-120-1 is a 16 channel, 3 tier QCB used in a DXL system to terminate audio field wiring (a single shielded twisted pair) for 400 series intercom stations and the audio cable (a single shielded twisted pair) for 300 series intercom stations.

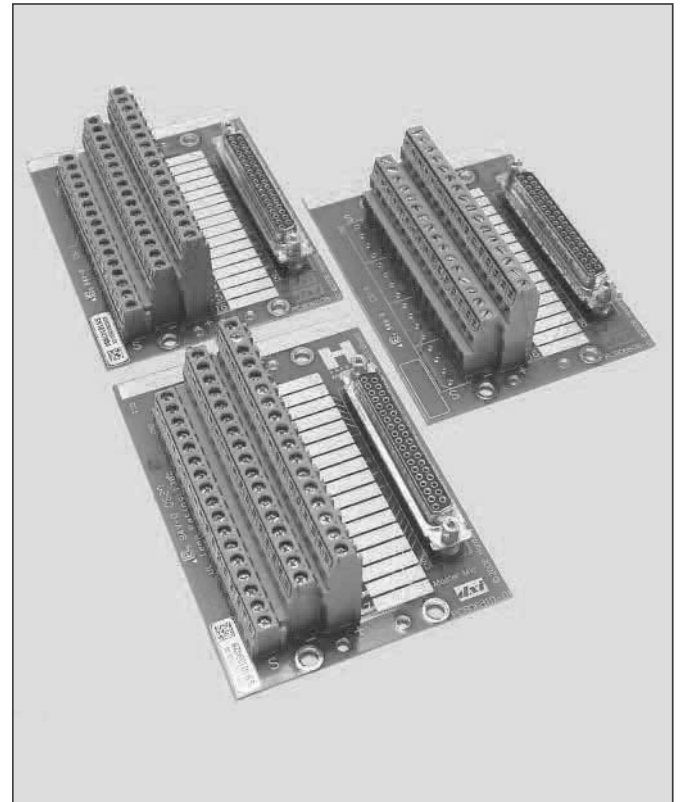
QCB-120-2 is a 16 channel, 2 tier QCB used for both DXL and DXI systems to terminate the switch field wiring (unshielded twisted pair) for 300 series intercom stations.

QCB-120-3 is a 17 channel, 3 tier QCB used in a DXI system to terminate the audio field wiring (a single shielded twisted pair) for 400 series intercom stations and 400 series master stations.

QCB-120-4 is a 16 channel, 3 tier QCB for use in both DXL and DXI systems to terminate the switch field wiring (two unshielded twisted pair) of 300 series intercom stations with two switches. The switch supervision resistors are included on the QCB-120-4.

### Features

- save costs with reduced field wiring time
- simplified interconnection reduces wiring errors
- all stations connected to numbered terminals and numbered designation strips
- simplified troubleshooting wiring faults
- designed to be backboard mounted, fit into standard 3.25 inch snap in track or mounted on a Din-rail



### Specifications

#### Physical Form Factor

QCB-120-1	3.25" x 4.28" x 1.50" (83 mm x 109 mm x 39 mm)
QCB-120-2	3.25" x 4.28" x 1.50" (83 mm x 109 mm x 39 mm)
QCB-120-3	3.25" x 4.52" x 1.50" (83 mm x 115 mm x 39 mm)
QCB-120-4	3.25" x 4.28" x 1.50" (83 mm x 109 mm x 39 mm)

#### Environmental

Operating Temperature	32 to 122 °F (0 to 50 °C)
Storage Temperature	-40 to 158 °F (-40 to 70 °C)
Humidity	0 to 95 % non-condensing

#### Field Connections

Intercom stations	screw clamp terminals
Exchange	double ended cable (DB 37 male connector at QCB)



## PowerEdge R360

Deliver powerful compute with a single processor server

The Dell PowerEdge R360 addresses evolving compute demands with an easy to manage rack server designed for businesses looking for affordable enterprise features.

### Elevate your enterprise to new heights with PowerEdge R360

Powered by the latest Intel® Xeon® E-2400 processors, Dell PowerEdge R360 is designed for productivity and data intensive applications, making it ideal for your growing business. With 4400/MT DDR5 and advanced NVMe BOSS-N1, it supports reduced latency and seamless scalability to bring the computing capability to the next level. Beyond the computing power, the Dell PowerEdge R360 is equipped with energy-efficient power supply, hot-plug storages, air cooling fans to make it a reliable, responsible, and secure choice.

### Enterprise-level GPU support

The PowerEdge R360 supports NVIDIA A2 GPU to meet the growing demand in video and audio computing. It provides cost-effective solutions for ROBO and Near-Edge customers from retail, manufacturing, and logistics.

This makes the PowerEdge R360 a powerful and versatile server for small to mid-sized businesses to enable a variety of workloads ranging from business-critical to cloud infrastructure. It is also widely used for point-of-sale transactions and enterprise level requirements for data analysis and virtualization.

### Cyber Resilient Architecture for Zero Trust IT environment & operations

Security is integrated into every phase of the PowerEdge lifecycle, including protected supply chain and factory-to-site integrity assurance. Silicon-based root of trust anchors end-to-end boot resilience while Multi-Factor Authentication (MFA) and role-based access controls ensure trusted operations.

### Increase efficiency and accelerate operations with autonomous collaboration

The Dell OpenManage systems management portfolio tames the complexity of managing and securing IT infrastructure. Using Dell Technologies' intuitive end-to-end tools, IT can deliver a secure, integrated experience by reducing process and information silos in order to focus on growing the business. The Dell OpenManage portfolio is the key to your innovation engine, unlocking the tools and automation that help you scale, manage, and protect your technology environment.

### Sustainability

From recycled materials in our products and packaging, to thoughtful, innovative options for energy efficiency, the PowerEdge portfolio is designed to make, deliver, and recycle products to help reduce the carbon footprint and lower your operation costs. We even make it easy to retire legacy systems responsibly with Dell Technologies.

### Services

Rest easier with Dell Technologies Services. Maximize your PowerEdge Servers with comprehensive services ranging from Consulting, to ProDeploy and ProSupport suites, Data Migration and more – available across 170 countries and backed by our 60K+ employees and partners.

### PowerEdge R360

The Dell PowerEdge R360 offers streamlined productivity, high-speed memory and capacity, and powerful compute to address common business applications. Ideal for inside or outside of the data center:

- Small to mid-sized businesses
- ROBO / Near-edge
- Collaboration and sharing
- Database support and management

Feature	Technical Specifications	
Processor	One Intel Xeon E-2400 series processor with up to 8 cores or One Intel Pentium G7400/G7400T processor with 2 cores	
Memory	<ul style="list-style-type: none"> <li>4 DDR5 DIMM slots, supports UDIMM 128 GB max, speeds up to 4400 MT/s</li> <li>Supports unregistered ECC DDR5 DIMMs only</li> </ul>	
Storage controllers	<ul style="list-style-type: none"> <li>Internal Controllers: HBA355i Adpt, PERC H355 Adpt, PERC H755 Adpt, HBA355i front, H355 front, H755 front</li> <li>Internal Boot: Internal USB 3.0, or Boot Optimized Storage Subsystem (BOSS-N1): HWRAID 2 x M.2 SSDs, USB</li> <li>External HBAs (non-RAID): HBA355e Adpt</li> <li>Software Controller: S160</li> </ul>	
Drive Bays	Front bays: <ul style="list-style-type: none"> <li>Up to 4 x 3.5-inch SAS/SATA (HDD/SSD) max 64 TB</li> <li>Up to 8 x 2.5-inch SAS/SATA (SSD) max 61.44 TB</li> </ul>	
Power Supplies	<ul style="list-style-type: none"> <li>600 W Platinum 100 — 240 VAC or 240 VDC, hot swap redundant</li> <li>700 W Titanium 200 — 240 VAC or 240 VDC, hot swap redundant</li> </ul>	
Cooling Options	Air cooling	
Fans	<ul style="list-style-type: none"> <li>Up to 4 fans</li> </ul>	
Dimensions	<ul style="list-style-type: none"> <li>Height – 42.8 mm (1.68 inches)</li> <li>Width – 482.0 mm (18.97 inches)</li> <li>Depth – 585.3 mm (23.04 inches) without bezel</li> <li>Depth — 598.9 mm (23.57 inches) with bezel</li> </ul>	
Form Factor	1U rack server	
Embedded Management	<ul style="list-style-type: none"> <li>iDRAC9</li> <li>iDRAC Direct</li> <li>iDRAC RESTful API with Redfish</li> <li>iDRAC Service Manual</li> </ul>	
Bezel	Security bezel	
OpenManage Software	<ul style="list-style-type: none"> <li>OpenManage Enterprise</li> <li>OpenManage Power Manager plugin</li> <li>OpenManage Service plugin</li> <li>OpenManage Update Manager plugin</li> <li>CloudIQ for PowerEdge plug in</li> <li>OpenManage Enterprise Integration for VMware vCenter</li> <li>OpenManage Integration for Microsoft System Center</li> <li>OpenManage Integration with Windows Admin Center</li> </ul>	
Mobility	OpenManage Mobile	
OpenManage Integrations	<ul style="list-style-type: none"> <li>BMC Truesight</li> <li>Microsoft System Center</li> <li>OpenManage Integration with ServiceNow</li> <li>Red Hat Ansible Modules</li> <li>Terraform Providers</li> <li>VMware vCenter and vRealize Operations Manager</li> </ul>	
Security	<ul style="list-style-type: none"> <li>Cryptographically signed firmware</li> <li>Data at Rest Encryption (SEDs with local or external key mgmt)</li> <li>Secure Boot</li> <li>Secured Component Verification (Hardware integrity check)</li> <li>Secure Erase</li> <li>Secured-core server</li> <li>Silicon Root of Trust</li> <li>System Lockdown (requires iDRAC9 Enterprise or Datacenter)</li> <li>TPM 2.0 FIPS, CC-TCG certified, TPM 2.0 China NationZ</li> </ul>	
Embedded NIC	2 x 1 GbE LOM	
GPU Options	1 x 60 W single-width GPU	
Ports	Front Ports <ul style="list-style-type: none"> <li>1 x iDRAC Direct (Micro-AB USB) port</li> <li>1 x USB 2.0</li> </ul>	Rear Ports <ul style="list-style-type: none"> <li>1 x Dedicated iDRAC Ethernet port</li> <li>1 x USB 2.0</li> <li>1 x USB 3.2 Gen1</li> <li>1 x VGA</li> <li>1 x Serial</li> </ul>
	Internal Ports <ul style="list-style-type: none"> <li>1 x USB 3.2 Gen1</li> </ul>	
PCIe	Up to two PCIe Gen4 slots on the Gen4 Riser <ul style="list-style-type: none"> <li>Slot 1: 1 x8 with x8 bandwidth, Half Length, Low Profile</li> <li>Slot 2: 1 x16 with x8 bandwidth, Half Length, Low Profile</li> <li>One dedicated PCIe x8 slot on the system board for internal PERC</li> </ul>	



Feature	Technical Specifications
Operating System and Hypervisors	<ul style="list-style-type: none"> <li>• Canonical Ubuntu Server LTS</li> <li>• Microsoft Windows Server with Hyper-V</li> <li>• Red Hat Enterprise Linux</li> <li>• SUSE Linux Enterprise Server</li> <li>• VMware ESXi</li> </ul> <p>For specifications and interoperability details, see <a href="http://Dell.com/OSsupport">Dell.com/OSsupport</a>.</p>
OEM-ready version available	From bezel to BIOS to packaging, your servers can look and feel as if they were designed and built by you. For more information, visit <a href="http://Dell.com/OEM">Dell.com/OEM</a> .

## APEX on Demand

APEX Flex on Demand Acquire the technology you need to support your changing business with payments that scale to match actual usage. For more information, visit [www.delltechnologies.com/en-us/payment-solutions/flexible-consumption/flex-on-demand.htm](http://www.delltechnologies.com/en-us/payment-solutions/flexible-consumption/flex-on-demand.htm).

### Discover more about PowerEdge servers



Learn more about  
services for  
PowerEdge servers



Learn more about our  
systems management  
solutions



Search our  
Resource Library



Follow PowerEdge  
servers on Twitter



Contact a Dell  
Technologies Expert  
for Sales or Support

# HP LaserJet Pro 4001 n/dn/dw Black & White Printer Series



Get blazing fast printing speeds and easy management tools with LaserJet Pro

Get blazing fast printing speeds and easy management tools with LaserJet Pro.

This printer is intended to work only with cartridges that have a new or reused HP chip, and it uses dynamic security measures to block cartridges using a non-HP chip. Periodic firmware updates will maintain the effectiveness of these measures and block cartridges that previously worked. A reused HP chip enables the use of reused, remanufactured, and refilled cartridges. More at: <http://www.hp.com/learn/ds>



HP LaserJet Pro 4001n Printer



HP LaserJet Pro 4001dn Printer



HP LaserJet Pro 4001dw Printer

## Maximum productivity

- Support your dynamic workteam with this high-speed printer, ideal for up to 10 users.
- Step up your workflow with blazing fast speeds to meet high-demand environments.
- Get productivity in the palm of your hand. Print and save time with Shortcuts from HP Smart.<sup>2</sup>
- Don't wait for print jobs. With no warm up time your printer is always ready.

## Seamless management.

- Centralize your print management. HP Web Jetadmin makes it easy with its suite of features.<sup>4</sup>
- Set up your printers quickly. Streamlined setup makes it easy to set up and get back to business
- Avoid interruptions with Wi-Fi<sup>®</sup> that automatically looks for the best connection to stay on-line.

## HP Wolf Pro Security.

- Get printer security out of the box. Preconfigured settings mean it's ready when you are.
- Add a layer of security. PIN/pull option authenticates your print jobs only when you're present.
- Set configuration policies and validate settings universally with HP Security Manager.<sup>9</sup>

<sup>1</sup>Measured using ISO/IEC 24734 and excludes first set of test documents. For more information, see [hp.com/go/printerclaims](http://hp.com/go/printerclaims). Exact speed varies depending on the system configuration, software application, driver, and document complexity.

<sup>2</sup>Requires HP app download available at [www.hp.com/go/mobileprinting](http://www.hp.com/go/mobileprinting). Certain features are available in English language only, and may vary by printer model/country, and between desktop/mobile applications. HP reserves the right to introduce charges for use of functionality facilitated by the HP app. Internet access required and may not be available in all countries. HP account required for full functionality. Fax capabilities are for sending a fax only. List of supported operating systems available in app stores. See details at [www.hp.com/go/mobileprinting](http://www.hp.com/go/mobileprinting).

<sup>4</sup>HP Web Jetadmin is available for download at no additional charge at [hp.com/go/webjetadmin](http://hp.com/go/webjetadmin).

<sup>5</sup>HP calculations based on ENERGY STAR<sup>®</sup> normalized TEC data comparing HP LaserJet 200-500 series printers at launch. See [hp.com/ecosmart](http://hp.com/ecosmart)

<sup>6</sup>HP Auto-On/Off Technology capabilities subject to printer and settings. may require a firmware upgrade.

<sup>7</sup>Recycling: Program availability varies. Original HP cartridge return and recycling is currently available in more than 60 countries, territories and regions in Asia, Africa, Europe, and North and South America through the HP Planet Partners program. For details, see [hp.com/recycle](http://hp.com/recycle).

<sup>8</sup>Internet access required and must be purchased separately. Wireless operations are compatible with 2.4 GHz and 5.0 GHz operations only. Supports both 5.0 GHz and 2.4 GHz using up to 12 non-overlapping channels vs. only 3 non-overlapping channels for 2.4 GHz only. Supports 5.0 GHz band (up to 150 mbps) v. 2.4 GHz band (up to 72.2 mbps). Learn more at: [www.hp.com/go/mobileprinting](http://www.hp.com/go/mobileprinting)

<sup>9</sup>HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit [hp.com/go/securitymanager](http://hp.com/go/securitymanager).

## Product walkaround

- 1. 100-sheet multipurpose tray 1 supports media sizes up to 8.5 x 14 inches (216 x 356 mm)
- 2. 2-line back lit LCD graphic display
- 3. 150-sheet output bin
- 4. Automatic two-sided printing
- 5. 250-sheet input tray 2 supports media sizes up to 8.5 x 14 inches (216 x 356 mm)



## Series at a glance



Model	HP LaserJet Pro 4001n Printer	HP LaserJet Pro 4001dn Printer	HP LaserJet Pro 4001dw Printer
Product number	Z2599F	Z2600F	Z2601F
Print speed (letter/A4)	Up to 42/40 pages per minute (ppm)		
Two-sided printing	N/A	√	
Control panel display	2-line back lit LCD graphic display		
100-sheet multipurpose tray 1, 250-sheet tray 2	√		
Optional 550-sheet tray 3	Add up to one (all models)		
Input capacity (standard/maximum)	Up to 350/900 sheets (all models)		
Recommended monthly page volume	Up to 750 to 4000 pages		
Cartridge yields (A/X/XC)	Black: ~2,900/9,500/10,000 pages		

## HP Services

Downtime can have serious consequences, so HP provides support beyond the standard warranty. You benefit from reduced risk, maximized uptime, predictable service delivery and no unbudgeted repair costs. HP Care Pack Services provide a comprehensive suite of protection services designed to keep HP hardware and software up and running so employees can stay productive.

For carepack availability visit: [hp.com/go/cpc](http://hp.com/go/cpc)



## Top features

Compact design with groundbreaking performance. High-speed, double-sided printing at up to 42 ppm and self-healing Wi-Fi®. HP Smart app enabled so you can easily print from your mobile devices.<sup>1,2</sup>

Manage your printers with the powerful Web Jetadmin. Intuitive management tools help you add and updates devices, solutions, and policies.<sup>3,4</sup>

Advance your security with HP Wolf Pro security—instantly embedded and preconfigured out of the box

### Accessories

**D9P29A** HP LaserJet Pro 550-sheet Feeder Tray

### Supplies

**W1020XC** HP W1020XC High Yield Black Contract Original LaserJet Toner Cartridge (~10,000) pages  
**W1480A** HP 148A Black Original LaserJet Toner Cartridge 1 Black (~2,900) pages  
**W1480X** HP 148X High Yield Black Original LaserJet Toner Cartridge 1 Black (~9,500) pages

### Solutions

**Workflow:** Scan Destinations

**Security:** HP Security Manager; Optional Smart Security; HP Secure Print and Insights

**Mobile and universal print:** HP Universal Print Driver (UPD); HP Print for Chrome Extension; Optional Print Anywhere with Private Pickup; Optional Smart Printing Driver; HP Smart UPD

**Management:** HP Web JetAdmin; HP Smart Device Services (SDS); HP Smart Admin; Embedded Web Server; HP Smart Printer Administrator's Resource Kit; HP Command Center 2.0(ECP); Premium Fleet & Security Management on ECP(Premium Experience)

### Services

**U42HDE** - HP 2 year Next Business Day Service for LaserJet Pro 400x

**U42HFE** - HP 3 year Next Business Day Service for LaserJet Pro 400x

**U42HGE** - HP 4 year Next Business Day Service for LaserJet Pro 400x

**U42HHE** - HP 5 year Next Business Day Service for LaserJet Pro 400x

**U42HJE** - HP 2 year 4 hour 9x5 Service for LaserJet Pro 400x

**U42HKE** - HP 3 year 4 hour 9x5 Service for LaserJet Pro 400x

**U42HLE** - HP 4 year 4 hour 9x5 Service for LaserJet Pro 400x

**U42HME** - HP 5 year 4 hour 9x5 Service for LaserJet Pro 400x

**U42HNE** - HP 3 year Next Business Day Advanced Exchange Service for LaserJet Pro 400x

**U42HQE** - HP 3 year Return to Depot Service for LaserJet Pro 400x

**U42HRPE** - HP 1 year Post Warranty Next Business Day Service for LaserJet Pro 400x

**U42HSPE** - HP 1 year Post Warranty 4 hour 9x5 Service for LaserJet Pro 400x

**U42HTPE** - HP 1 year Post Warranty Next Business Day Advanced Exchange Service for LaserJet Pro 400x

**U42HVPE** - HP 1 year Post Warranty Return to Depot Service for LaserJet Pro 400x

**U9JT1E** - HP Installation with Networking Service for Personal Scanner and Printing

<sup>1</sup> Measured using ISO/IEC 24734 and excludes first set of test documents. For more information, see [hp.com/go/printerclaims](http://hp.com/go/printerclaims). Exact speed varies depending on the system configuration, software application, driver, and document complexity.

<sup>2</sup> Requires HP app download available at [www.hp.com/go/mobileprinting](http://www.hp.com/go/mobileprinting). Certain features are available in English language only, and may vary by printer model/country, and between desktop/mobile applications. HP reserves the right to introduce charges for use of functionality facilitated by the HP app. Internet access required and may not be available in all countries. HP account required for full functionality. Fax capabilities are for sending a fax only. List of supported operating systems available in app stores. See details at [www.hpsmart.com](http://www.hpsmart.com).

<sup>3</sup> HP Web Jetadmin is available for download at no additional charge at [hp.com/go/webjetadmin](http://hp.com/go/webjetadmin).

<sup>4</sup> HP calculations based on ENERGY STAR® normalized TEC data comparing HP LaserJet 200-500 series printers at launch. See [hp.com/ecosmart](http://hp.com/ecosmart)

<sup>5</sup> HP Auto-On/Auto-Off Technology capabilities subject to printer and settings; may require a firmware upgrade.

<sup>7</sup> Recycling: Program availability varies. Original HP cartridge return and recycling is currently available in more than 60 countries, territories and regions in Asia, Africa, Europe, and North and South America through the HP Planet Partners program. For details, see [hp.com/recycle](http://hp.com/recycle).

<sup>8</sup> Internet access required and must be purchased separately. Wireless operations are compatible with 2.4 GHz and 5.0 GHz operations only. Supports both 5.0 GHz and 2.4 GHz using up to 12 non-overlapping channels vs. only 3 non-overlapping channels for 2.4 GHz only. Supports 5.0 GHz band (up to 150 mbps) v. 2.4 GHz band (up to 72.2 mbps). Learn more at: [www.hp.com/go/mobileprinting](http://www.hp.com/go/mobileprinting)

<sup>9</sup> HP JetAdvantage Security Manager must be purchased separately. To learn more, please visit [hp.com/go/securitymanager](http://hp.com/go/securitymanager).

# SQL SERVER 2022 LICENSING DATASHEET

## Editions overview

The SQL Server 2022 editions align with how customers are deploying applications and solutions:

- **Enterprise Edition** is ideal for applications requiring mission critical in-memory performance, security, and high availability
- **Standard Edition** delivers fully featured database capabilities for mid-tier applications and data marts

SQL Server 2022 is also available in free Developer and Express editions. Web Edition is offered in the Services Provider License Agreement (SPLA) program only.

## SQL Server 2022 licensing models

SQL Server 2022 offers customers a variety of licensing options aligned with how customers typically purchase specific workloads. There are two main licensing models that apply to SQL Server:

**PER CORE:** Gives customers a more precise measure of computing power and a more consistent licensing metric, regardless of whether solutions are deployed on physical servers on-premises, or in virtual or cloud environments.

- Core based licensing is appropriate when customers are unable to count users/devices, have Internet/Extranet workloads or systems that integrate with external facing workloads.
- Under the Per Core model, customers license either by physical server (based on the full physical core count) or by virtual machine (based on virtual cores allocated), as further explained below.

**SERVER + CAL:** Provides the option to license users and/or devices, with low-cost access to incremental SQL Server deployments.

- Each server running SQL Server software requires a server license.
- Each user and/or device accessing a licensed SQL Server requires a SQL Server CAL that is the same version or newer – for example, to access a SQL Server 2019 Standard Edition server, a user would need a SQL Server 2019 or 2022 CAL.

- Each SQL Server CAL allows access to multiple licensed SQL Servers, including Standard Edition and legacy Business Intelligence and Enterprise Edition Servers.

## SQL Server 2022 Editions availability by licensing model:

SQL Server 2022 Edition	Licensing Options	
	Server + CAL	Per Core
Enterprise		•
Standard	•	•
Developer	Free edition	
Express	Free edition	

## Benefits of SQL Server 2022 with SA or Subscription Licenses

Software Assurance coverage and subscription licenses help customers take full advantage of their SQL Server license investment. With SA or subscription licenses, SQL Server customers unlock valuable benefits including:

Software Assurance Benefit	SQL Server 2022 Editions	
	Standard	Enterprise
Azure Hybrid Benefit	•	•
Fail-Over servers for disaster recovery	•	•
Fail-Over servers for disaster recovery in Azure	•	•
Fail-Over servers for high availability	•	•
Unlimited virtualization (VMs)		•
Unlimited containers	Yes	Yes
Option to license by virtual machine	•	•
Power BI Report Server		•

By combining mission critical performance, scale and availability of SQL Server Enterprise Edition with the benefits provided through SA or subscription licenses, customers unlock the full power of SQL Server:

- Stay current with all SQL Server features
- Access an unlimited number of virtual machines

# SQL SERVER 2022 LICENSING DATASHEET

- Modernize to the cloud with existing licenses
- Take advantage of high availability scenarios at no additional licensing cost
- Generate data visualizations on premises with Power BI Report Server




## Licensing for virtualization and containers

SQL Server 2022 offers use rights for virtual machines and containers, to provide flexibility for customers' deployments. There are two primary licensing options for virtual machines and containers in SQL Server 2022 – the ability to license individual virtual machines and containers and the ability to license for maximum densities in highly virtualized or high-density container environments.






### INDIVIDUAL VIRTUAL MACHINES OR CONTAINERS

As hardware capabilities grow, it continues to be more common for each database to use a fraction of its server's computing power. When deploying databases on Virtual Machines (VMs) or containers that use just a fraction of a physical server, savings can be achieved by licensing individual VMs or containers. Licensing SQL Server 2022 by VM or container is an option under core subscription licenses or licenses with SA only.

**Note:** For licensing, Containers follow the same rules as licensing SQL Server for virtual machines.

				
Virtual cores	2	4	6	
Licenses	4	4	6	<b>14</b> Total core licenses Purchase seven 2-pack SKUs of core licenses

This figure illustrates the licensing requirements for three different virtual machines under the Per Core licensing model.

					
Server licenses	1	1			<b>2</b> Total server licenses
Client access licenses			1	1	<b>3</b> Total CAL licenses

This figure shows an example of licensing virtual machines under the Server+CAL licensing model.

Note: When licensing VMs or containers under the Server + CAL model, the number of virtual or physical cores does not affect the number of server licenses required.

- To license a VM or container with core licenses, purchase a core subscription license or license with SA for each virtual core (virtual thread) allocated to the VM or the number of cores configured for access by the container (with a minimum of 4 licenses per VM or container).
- To license a single VM or container with a server license (for Standard Edition only), purchase a server license for each VM or container, and a CAL for each user or device.
- Each VM or container covered with subscription licenses or licenses with SA can be moved frequently within a server farm, or to a third-party hoster or cloud services provider\*, without the need to purchase additional SQL Server licenses.

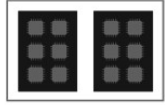
\*Customers can use Authorized Mobility Partners under licenses with SA (via License Mobility through SA) or Authorized Outsourcers under subscription licenses or licenses with SA (via the Flexible Virtualization Benefit). See <https://www.microsoft.com/licensing/terms/productoffering> for details.

## HIGH-DENSITY VIRTUALIZATION OR CONTAINER DEPLOYMENT

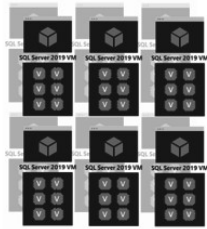
Further savings can be achieved by licensing SQL Server high density VM or container deployments. This is a great option for customers who want to take advantage of the full computing power of their physical servers and have very dynamic provisioning and de-provisioning of virtual resources or container images.

# SQL SERVER 2022 LICENSING DATASHEET

License all physical cores in the server



Deploy unlimited VMs



Physical cores	6	6	12	Total physical cores
Core licenses	6	6	12	Total core licenses

Shown is an example of licensing a 12-core physical server for unlimited VMs with Enterprise Edition core licenses and SA.

## Physical core licensing – Enterprise Edition

- Customers can deploy an unlimited number of VMs or containers on the server and utilize the full capacity of the licensed hardware, by fully licensing the server (or server farm) with Enterprise Edition core subscription licenses or licenses with SA coverage based on the total number of physical cores on the servers.
- Subscription licenses or SA provide(s) the option to run an unlimited number of virtual machines or containers to handle dynamic workloads and fully utilize the hardware's computing power.

## Virtual core licensing – Standard/Enterprise Edition

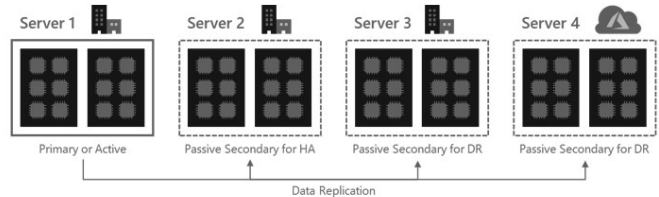
- When licensing by virtual core on a virtual OSE with subscription licenses or SA coverage on all virtual cores (including hyperthreaded cores) on the virtual OSE, customers may run any number of containers in that virtual OSE. This benefit applies both to Standard and Enterprise Edition.

## Licensing for high availability and Disaster Recovery

SQL Server software can be configured so that if one server or VM fails, its processing will be picked up, recovered and continued by another server or VM. Under SQL Server 2022 subscription licenses or licenses with active SA, customers can use the following passive replicas in conjunction with their primary workloads in anticipation of a failover event:

- One passive fail-over replica for High Availability in a separate server or VM
- One passive fail-over replica for Disaster Recovery in a separate server or VM

- One passive fail-over replica for Disaster Recovery in a single VM on Azure



Active cores	12		48	Total cores
Passive cores		36		
Core licenses	12	0	12	Total core licenses Purchase six 2-pack SKUs of core licenses

These passive fail-over rights apply to workloads running on a customer's own servers and workloads a customer deploys on an Authorized Outsourcer's servers. Customers deployed in Azure or with Authorized License Mobility partners have different passive fail-over rights. See the [Product Terms](#) for details.

## Licensing for non-production use

SQL Server 2022 Developer Edition provides a fully featured version of SQL Server software—including all the features and capabilities of Enterprise Edition—licensed for development, test and demonstration purposes only.

Customers may install and run the SQL Server Developer Edition software on any number of devices. This is significant because it allows customers to run the software on multiple devices (for testing purposes, for example) without having to license each non-production server system for SQL Server.

A production environment is defined as an environment that is accessed by end-users of an application (such as an Internet website) and that is used for more than gathering feedback or acceptance testing of that application.

SQL Server 2022 Developer Edition is a free product, available for download at the SQL Server Application Development site: [aka.ms/SQLServerAppDev](https://aka.ms/SQLServerAppDev)

Developers can also gain access to SQL Server Developer through the Visual Studio Dev Essentials program, which also provides access to many other valuable developer resources. For more information visit: [aka.ms/VisualStudioDev](https://aka.ms/VisualStudioDev)

## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: Lt. Scott Brown (Name of Person completing survey)

Madison County Sheriff's Office (Name of Client Company/Consultant)

Phone Number: 256-519-4845 Email: sbrown@madisoncountyal.gov

Subject: Past Performance Survey of Similar work:

Project name: Madison County Sheriff's Office

Name of Vendor being surveyed: Driven Security LLC

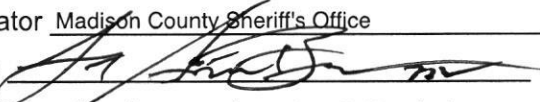
Cost of Services: Original Cost: 1,600,000 Ending Cost: 1,600,000

Contract Start Date: 9/20/2020 Contract End Date: 4/16/2025

**Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.**

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	10
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	10
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator Madison County Sheriff's Office

Signature of Evaluator: 

Please fax or email the completed survey to: adam@drivenlocks.com



## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: David Hochgraber (Name of Person completing survey)

Adams County Illinois (Name of Client Company/Consultant)

Phone Number: 217-277-2161 Email: dhochgraber@co.adams.il.us

Subject: Past Performance Survey of Similar work:

Project name: Adams County

Name of Vendor being surveyed: Driven Security LLC

Cost of Services: Original Cost: 910,000 Ending Cost: 910,000

Contract Start Date: 1/27/2023 Contract End Date: 4/16/2025

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	10
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	10
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator David Hochgraber

Signature of Evaluator: 

Please fax or email the completed survey to: adam@drivenlocks.com

## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: Patrick Sutton (Name of Person completing survey)

Marion County Schools (Name of Client Company/Consultant)

Phone Number: 205-412-6859 Email: psutton@mcbe.net

Subject: Past Performance Survey of Similar work:

Project name: Marion County Schools

Name of Vendor being surveyed: Driven Security LLC

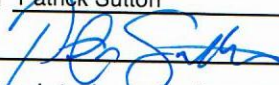
Cost of Services: Original Cost: 1,600,000 Ending Cost: 1,600,000

Contract Start Date: 9/30/2024 Contract End Date: 12/31/2024

Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	9
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	9
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator Patrick Sutton

Signature of Evaluator: 

Please fax or email the completed survey to: adam@drivenlocks.com

## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: Maggie Stampley (Name of Person completing survey)

Lead Schools (Name of Client Company/Consultant)

Phone Number: (615) 800-8293 Email: maggie.stampley@leadpublicschools.org

Subject: Past Performance Survey of Similar work:

Project name: Lead Schools

Name of Vendor being surveyed: Driven Security

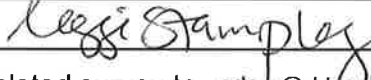
Cost of Services: Original Cost: 700,000 Ending Cost: 700,000

Contract Start Date: 4/1/2024 Contract End Date: 2/1/

**Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.**

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	10
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	10
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator Maggie Stampley

Signature of Evaluator: 

Please fax or email the completed survey to: adam@drivenlocks.com

## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: Jason Gardner (Name of Person completing survey)

Swain County North Carolina (Name of Client Company/Consultant)

Phone Number: 828-488-0159 Email: jbgardner@swaincountync.gov

Subject: Past Performance Survey of Similar work:

Project name: Swain County

Name of Vendor being surveyed: Driven Security LLC

Cost of Services: Original Cost: 261,000 Ending Cost: 261,000

Contract Start Date: 8/1/2024 Contract End Date: 10/1/2024

**Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.**

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	10
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	10
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator: Jason Gardner

Signature of Evaluator: 

Please fax or email the completed survey to: adam@drivenlocks.com

## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: David Thompson (Name of Person completing survey)

Buncombe County North Carolina (Name of Client Company/Consultant)

Phone Number: (828) 775 - 6704 Email: David.Thompson@buncombenc.gov

Subject: Past Performance Survey of Similar work:

Project name: Buncombe County North Carolina

Name of Vendor being surveyed: Driven Security LLC via The Graceway Group LLC

Cost of Services: Original Cost: 612,000 Ending Cost: 612,000

Contract Start Date: 2/12/2023 Contract End Date: 11/1/2023

**Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.**

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	10
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	10
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator David Thompson

Signature of Evaluator: David A. Thompson 

Please fax or email the completed survey to: adam@drivenlocks.com

## Survey Questionnaire – Polk County

### RFP 25-191, Polk County South & Central County Jail Security Upgrades

To: Wendy Cochran (Name of Person completing survey)

Auburn Housing Authority (Name of Client Company/Consultant)

Phone Number: (334) 821-2262 ext 228 Email: wcochran@auburnhousingauth.org

Subject: Past Performance Survey of Similar work:

Project name: Auburn Housing Authority

Name of Vendor being surveyed: Driven Security

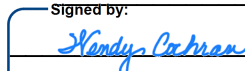
Cost of Services: Original Cost: 400,000 Ending Cost: 400,000

Contract Start Date: 9/1/2020 Contract End Date: 4/1/2025

**Rate each of the criteria on a scale of 1 to 10, with 10 representing that you were very satisfied (and would hire the Consultant /individual again) and 1 representing that you were very unsatisfied (and would never hire the Consultant /individual again). Please rate each of the criteria to the best of your knowledge. If you do not have sufficient knowledge of past performance in a particular area, leave it blank.**

NO	CRITERIA	UNIT	SCORE
1	Ability to manage cost	(1-10)	10
2	Ability to maintain project schedule (complete on-time/early)	(1-10)	10
3	Quality of workmanship	(1-10)	10
4	Professionalism and ability to manage	(1-10)	10
5	Close out process	(1-10)	10
6	Ability to communicate with Client's staff	(1-10)	10
7	Ability to resolve issues promptly	(1-10)	10
8	Ability to follow protocol	(1-10)	10
9	Ability to maintain proper documentation	(1-10)	10
10	Appropriate application of technology	(1-10)	10
11	Overall Client satisfaction and comfort level in hiring	(1-10)	10
12	Ability to offer solid recommendations	(1-10)	10
13	Ability to facilitate consensus and commitment to the plan of action among staff	(1-10)	10

Printed Name of Evaluator Wendy Cochran

Signature of Evaluator: 

Please fax or email the completed survey to: adam@drivenlocks.com