



(SOC) 3 Report

System and Organization Control (SOC) 3 Report

Report on Kuberno Limited's Kube Cloud Platform Relevant to Security

For the period December 1, 2024 to November 30, 2025



ZeroDayCPA

Table of Contents

Independent Service Auditor’s Report	4
Kuberno Limited’s Management Assertion	8
Software	11
Data	12
People	12
Policies	12
Control Environment	14
Risk Assessment Process	14
Monitoring, Logging, and Alerting Activities	15
Complementary User Entity Controls	16
Subservice Organizations	17





Section 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Kuberno Limited,

Scope

We have examined Kuberno Limited's (Kuberno's) accompanying assertion, titled "Kuberno Limited's Management Assertion" (assertion) that the controls within Kuberno's Kube Cloud Platform (system) were effective throughout the period December 1, 2024 to November 30, 2025 to provide reasonable assurance that Kuberno'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).

Kuberno uses the subservice organizations described in the "Subservice Organizations" subsection of Attachment A of the report. The information included within the Boundaries of Kuberno's System (Attachment A) indicates that Kuberno's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if the controls at the subservice organizations, assumed in the design of Kuberno's controls, are suitably designed and operating effectively along with the related controls at the service organization. The information included within the boundaries of the system presents Kuberno's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations and we have not evaluated whether the controls management assumes have been implemented at the subservice organization or whether such controls were suitably designed and operating effectively throughout the period December 1, 2024 to November 30, 2025.

The information included within the Boundaries of Kuberno Limited's System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Kuberno, to achieve the service commitments and system requirements of Kuberno based on the applicable trust services criteria. 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.

Service Organization's Responsibilities

Kuberno 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 Kuberno's service commitment and system requirements were achieved. Kuberno has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Kuberno is responsible for selecting and identifying in its assertion the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective through the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with the attestation standard established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether Management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the controls were not effective to achieve Kuberno's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Kuberno's service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

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 and 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.

Opinion

In our opinion, management's assertion that the controls within Kuberno's Kube Cloud Platform were effective throughout the period December 1, 2024 to November 30, 2025 to provide reasonable assurance that Kuberno's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

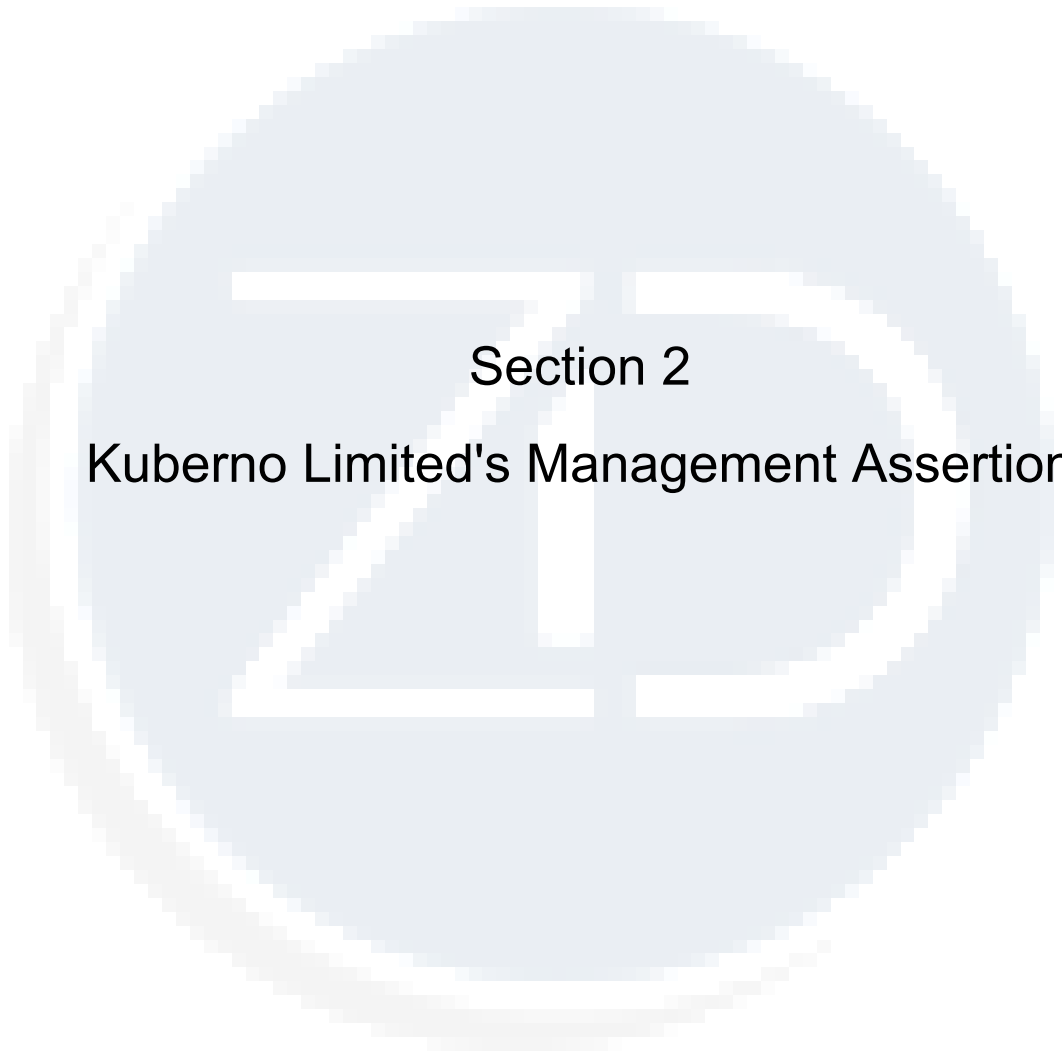
Zero Day CPA

Zero Day CPA, PC

July 20, 2026

Troy, Michigan





Section 2

Kuberno Limited's Management Assertion

Kuberno Limited's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Kuberno Limited's (Kuberno's) Kube Cloud Platform throughout the period December 1, 2024 to November 30, 2025 to provide reasonable assurance that Kuberno'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 section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

The information included within the Boundaries of Kuberno Limited's System (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Kuberno, to achieve Kuberno's service commitments and system requirements based on the applicable trust services criteria. The Boundaries of Kuberno Limited's System (Attachment A) presents the types of complementary subservice organisation controls assumed in the design of Kuberno's controls, and does not disclose the actual controls at the subservice organizations.

The information included within the Boundaries of Kuberno Limited's System (Attachment A) indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Kuberno, to achieve the service commitments and system requirements of Kuberno based on the applicable trust services criteria. Attachment A presents those complementary user entity controls assumed in the design of Kuberno's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2024 to November 30, 2025 to provide reasonable assurance that Kuberno's service commitments and system requirements would be achieved based on the applicable trust services criteria, if user entities and the subservice organizations applied the complementary controls assumed in the design of Kuberno's controls throughout that period. Kuberno's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2024 to November 30, 2025 to provide reasonable assurance that Kuberno's service

commitments and system requirements were achieved based on the applicable trust services criteria.

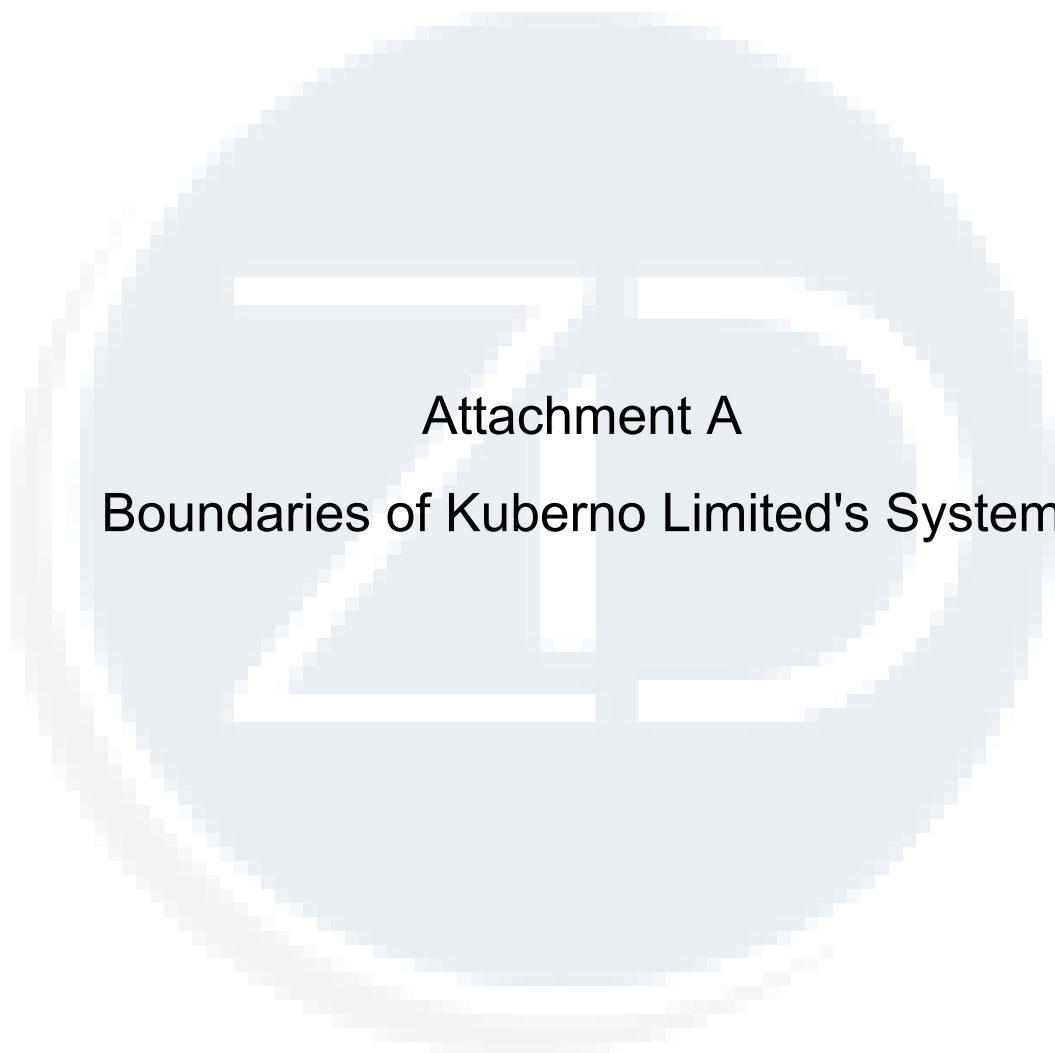
Attachment A

Boundaries of Kuberno Limited's system

Attachment B

Kuberno Limited's Service Commitments and System Requirements





Kuberno Limited's Kube Cloud Platform

Overview of the Company and the Types of Services Provided

Kuberno Limited's ("Kuberno" or "the Company") Kube Cloud Platform is designed to be the single source of truth around entity data, providing data insights and analysis through powerful reporting functionality and an intuitive user interface that means all stakeholders across executive teams, legal, tax, finance, compliance as well as the Company or corporate secretary and corporate governance functions can gain effective oversight over entity management direct to their screens-significantly reduce the time taken and improving the accuracy of regulatory and statutory reporting. Kube also streamlines entity compliance and governance processes through automation and workflows, as well as providing secretariat practice management functionality through dashboards that all combine to support more efficient Company Secretariat teams.

Components of the System

Infrastructure

The components that directly support the services provided to user entities are as follows:

Component	Description	Location
Kube Platform	End User Web Application wherein customer can input and view legal entity data	Azure
Company Registrar Integrations	Allows legal entity data to be integrated from the Company's registrar	Azure
Third Party Integrations	Allows legal entity data to be integrated from third parties	Azure

Software

The software component consists of the applications, programs, and other software that support the system. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Kube Cloud Platform are the following:

Function	Software Utilized
Version Control Tool	GitHub, Microsoft Visual Studio and Dependabot
Ticketing	Azure DevOps
Monitoring, Logging, and Alerting	Azure Monitor
Vulnerability Scanning and Management	Dependabot and Acunetix
Mobile Device Management (MDM)	Intune
Authentication	Microsoft 365
Human Resources	Rippling

Data

Data is stored in Azure SQL Servers and Azure Storage Accounts, and is ingested through integrations and end user input into the client web portal. The aforementioned databases, which house sensitive customer data, are encrypted at rest and sensitive data is not transmitted outside of Kuberno's environment. When the Company does transmit sensitive and confidential data over public networks it utilizes TLS/SSL. The Company also ensures that all in-scope production infrastructure and cloud resources containing customer data are configured to restrict public access without authentication.

People

Kuberno's organizational structure provides a framework for achieving and ensuring that entity-wide objectives are planned, executed, controlled and monitored.

Policies

The following provides a summary of Kuberno's policies and procedures that comprise the internal control for the system.

Policy	Purpose
Acceptable Use Policy	Defines standards for appropriate and secure use of company hardware and electronic systems, including storage media, communication tools, and internet access. This policy is acknowledged by employees and contractors upon hire.
Access Control and Termination Policy	Governs authentication and access to applications, resources, and tools.
Business Continuity and Disaster Recovery Policy	Governs required processes for restoring the service or supporting infrastructure after suffering a disaster or disruption.
Change Management Policy	Governs the documentation, tracking, testing, and approval of system, network, security, and infrastructure changes for applications, resources, and tools.
Code of Conduct	Outlines ethical expectations, behavior standards, and ramifications of non-compliance. This policy is acknowledged by employees and contractors upon hire.
Configuration and Asset Management Policy	Governs configurations for new applications, resources, and tools.
Encryption and Key Management Policy	Supports the requirements for secure encryption and decryption of app secrets and governs the use of cryptographic controls.
Information Security Policy	Establishes the security requirements for maintaining the security of applications, resources, and tools.
Internal Control Policy	Identifies how a system of controls should be maintained to safeguard assets, promote operational efficiency, and encourage adherence to prescribed managerial policies.
Network Security Policy	Identifies the requirements for protecting information and systems within and across networks.
Performance Review Policy	Provides personnel context and transparency into their performance and career development processes.
Risk Assessment and Treatment Policy	Governs the process for conducting risk assessments to account for threats, vulnerabilities, likelihood, and impact with respect to assets, team members, customers, vendors, suppliers, and partners.
Secure Development Policy	Defines the requirements for secure software and system development and maintenance.

Policy	Purpose
Security Incident Response Plan	Outlines the process of identifying, prioritizing, communicating, assigning, and tracking confirmed incidents through to resolution.
Vendor Management Policy	Defines a framework for the onboarding and management of the vendor relationship cycle.
Vulnerability Management and Patch Management Policy	Outlines the processes to identify and respond to vulnerabilities.

Control Environment

Kuberno's control environment reflects the philosophy of senior management concerning the importance of the security of data and information within that system. Kuberno's Security Steering Committee meets quarterly and oversees the security activities of Kuberno. The committee is charged with establishing overall security policies and procedures for Kuberno, including those related to the protection of confidential information. The importance of security is emphasized within Kuberno through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, Kuberno has taken operations staff that provide the day-to-day services into consideration for the relevance of controls to achieve the organization's service commitments and system requirements based on the applicable trust services criteria.

Risk Assessment Process

Kuberno has defined a risk management framework for evaluating information security risk and other relevant forms of business risk. Management performs a formal risk assessment at least annually to identify, update, assess and mitigate relevant internal and external threats related to security, along with the potential for fraud. A risk register is maintained during this risk assessment process to ensure that risk mitigation strategies for identified risks are tracked, and that any modified controls are consistent with the risk mitigation strategy.

As the Company places a heavy reliance on outside vendors for critical infrastructure, business functions, and processing capabilities, the Company has developed a Vendor Management Policy that establishes the compliance and performance expectations required of vendors, and the necessary due diligence and monitoring expectations required of the Company's personnel. Agreements, which include security requirements, are executed with vendors in accordance with the Vendor Management Policy. To ensure vendors are monitored periodically, Kuberno collects and reviews the compliance reports for its high-risk vendors on at least an annual basis.

Monitoring, Logging, and Alerting Activities

Kuberno performs monitoring in several different ways to assess and ensure the security and health of relevant in-scope tools, technologies, infrastructure and their related controls. The Company leverages a continuous monitoring solution which monitors internal controls used in the achievement of service commitments and system requirements. The tool identifies instances of non-compliance, which Management then resolves.

Logging is enabled and monitoring software is configured to collect metrics from ingested logs to detect potential security threats, unusual system activity, and monitor system performance, as applicable. Alerting software is used to notify impacted teams of potential security events, and identified events are tracked to resolution. To ensure potential security threats and other relevant security topics are discussed regularly, Management convenes a Security Steering Committee on a quarterly basis.

Incident Response

The Company utilizes multiple avenues to identify and alert potential security incidents, which were described in the *Communication and Monitoring, Logging, and Alerting* sections above. Confirmed incidents are documented and tracked according to the Security Incident Response Plan. If applicable following an incident, a 'lessons learned' document is created and shared with relevant personnel to ensure that any necessary updates to the policy or procedures are updated. To ensure personnel are familiar with, and comfortable executing the steps in this plan, Management performs an annual security incident response tabletop exercise.

Complementary User Entity Controls

User entities are responsible for their own control environments and their operational effectiveness. The following user entity controls are assumed to be implemented by user entities and are necessary for the service organization's service commitments and system requirements to be achieved.

User Entity Control	Relevant Criteria
User entities are responsible for setting up, monitoring, and removing user entity access to the system and ensuring that it is appropriate.	CC 6.1, CC 6.2, CC 6.3, CC 6.6
User entities are responsible for immediately notifying Kuberno of any actual or suspected information security breaches, including compromised user accounts.	CC 2.2, CC 2.3
User entities are responsible for ensuring the supervision, management, and control of the use of Kuberno services by their personnel.	CC 4.2
User entities are responsible for ensuring that only authorized and properly trained personnel are allowed access to the Kuberno services.	CC 5.3
User entities are responsible for adding access for Kuberno personnel for support for their instance, and removing the access when no longer needed.	CC 6.1, CC 6.2, CC 6.3, CC 6.6

Subservice Organizations

The Company utilizes the subservice organization in the following tables to achieve its objectives.

Subservice Organization	Services Provided
Microsoft Corporation (Azure)	The subservice organization provides the Company with cloud infrastructure. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization has implemented strong password requirements for authentication into its systems (CC 6.1, CC 6.6).
- The subservice organization ensures that logical access to infrastructure is restricted to appropriate personnel (CC 6.1, CC 8.1).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1, CC 6.7).
- The subservice organization ensures that data moving to and from its systems is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents. Additionally, the subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.1, CC 7.2, CC 7.3, CC 7.4, CC 7.5).

Subservice Organization	Services Provided
GitHub, Inc.	The subservice organization provides the Company with cloud-based source control software. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization has implemented strong password requirements for authentication into its systems (CC 6.1, CC 6.6).
- The subservice organization ensures that logical access to infrastructure is restricted to appropriate personnel (CC 6.1, CC 8.1).
- The subservice organization ensures that strong encryption keys are used to protect customer content and that master keys used for cryptographic operations are logically secured (CC 6.1, CC 6.7).

Subservice Organization	Services Provided
GitHub, Inc.	The subservice organization provides the Company with cloud-based source control software. This organization was carved out of the report.

Complementary Subservice Organization Controls

- The subservice organization ensures that data moving to and from its systems is encrypted in transit (CC 6.6, CC 6.7).
- The subservice organization ensures that physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual (CC 6.4).
- The subservice organization has implemented monitoring to identify and notify personnel of potential issues and/or incidents. Additionally, the subservice organization has implemented incident response procedures to identify, track, and respond to incidents (CC 7.1, CC 7.2, CC 7.3, CC 7.4, CC 7.5).





Attachment B

Kuberno Limited's Service Commitments and System Requirements

Kuberno Limited's Service Commitments and System Requirements

Kuberno designs its processes and procedures related to the Kube Cloud Platform to meet its objectives for its Kube Cloud Platform. Those objectives are based on the service commitments that Kuberno makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that Kuberno has established for the services.

Service commitments are declarations made by management to its customers regarding the performance of the Kube Cloud Platform. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offering provided online and consist of the following:

- Requires team members to review and accept all of the relevant security policies.
- The Company undergoes external third-party penetration testing at least annually to ensure there are no compromisable vulnerabilities.
- Requires team members to go through annual security awareness training relating to information security practices.
- Requires team members to go through a background check in accordance with local laws and regulations.
- Encrypts all databases at rest.
- Encrypts all data in transit.
- Performs vulnerability scanning and monitors for possible security threats.
- Performs monitoring and logging for cloud services.
- Establishes a process for handling information security events, which includes containment, mitigation, and communication procedures.
- Follows the principle of least privilege with respect to access management.
- Requires all team-members to adhere to a minimum set of password configurations and utilize MFA and SSO where applicable.
- Performs periodic user access reviews to ensure the appropriateness of all users.
- Requires all devices that are accessing client data to be enrolled in MDM tooling to ensure strong password configurations, anti-virus, and hard drive encryption configurations are enforced.
- Implements firewalls and network intrusion detection tools.

Kuberno establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- User Access Reviews
- Employee access provisioning and deprovisioning standards
- Encryption standards for data at rest and in transit
- Risk assessment standards
- Change management controls
- Incident Response Plan



CERTIFICATE *of* SIGNATURE

REF. NUMBER
VMEFG-PSNED-45JAS-7DZKR

DOCUMENT COMPLETED BY ALL PARTIES ON
20 JUL 2026 16:18:03
UTC

SIGNER

LANCE SAMONA

EMAIL
LANCE@ZERODAYCPA.COM

TIMESTAMP

SENT
20 JUL 2026 15:44:31

VIEWED
20 JUL 2026 16:17:34

SIGNED
20 JUL 2026 16:18:03

SIGNATURE

Zero Day CPA

IP ADDRESS
152.160.27.165

LOCATION
SOUTHFIELD, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
20 JUL 2026 16:17:34

