LOCKT™

SOC 2® Type 1 Report

Controls Related to Security

As of September 24, 2025

Prepared in accordance with the attestation standards established by the American Institute of Certified Public Accountants

mjd ADVISORS

AICPA SOC aicpa.org/soc4so SOC for Service Organizations™

Table of Contents

Section 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of Lockt, LLC
Houston, Texas

Scope

We have examined Lockt, LLC's (Lockt or the Company) accompanying description in Section 3 titled "Management's Description of the Lockt Platform" as of September 24, 2025 (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 of controls stated in the description as of September 24, 2025, to provide reasonable assurance that the Company'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)*.

The Company uses a subservice organization to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to ensure the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion in Section 2 titled "Assertion of Lockt, LLC Management" (assertion) about the description. The Company 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 the suitability of the design of controls stated in the description based on our examination. Our examination was conducted following attestation standards established by the AICPA. 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 were suitably designed to provide reasonable assurance the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

An examination of a description of a service organization's system and the suitability of the design of controls involves the following:

- 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
- 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 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 report 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. The projection to the future of any conclusions about the suitability of the design 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.

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and do not express an opinion thereon.

Opinion

In our opinion, in all material respects:

a) The description presents the Lockt Platform that was designed and implemented as of September 24, 2025, in accordance with the description criteria.

b) The controls stated in the description were suitably designed as of September 24, 2025, to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date and subservice organization applied the complementary controls assumed in the design of the Company's controls as of that date.

Restricted Use

This report is intended solely for the information and use of the Company, user entities of the Lockt Platform as of September 24, 2025, business partners of the Company subject to risks arising from interactions with the Lockt Platform, 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 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 the specified parties.

MJD Advisors

Waukee, Iowa
September 24, 2025

Section 2

Management's Assertion

Assertion of Lockt, LLC Management

Management of Lockt, LLC has prepared the accompanying description titled “Management’s Description of the Lockt Platform” as of September 24, 2025 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*. The description is intended to provide report users with information about the Lockt Platform that may be useful when assessing the risks arising from interactions with the Lockt Platform, particularly information about system controls the Company 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 set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The Company uses a subservice organization to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company’s service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company’s controls. The description does not disclose the actual controls at the subservice organization.

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

a) The description presents the Lockt Platform that was designed and implemented as of September 24, 2025, in accordance with the description criteria.

b) The controls stated in the description were suitably designed as of September 24, 2025, to provide reasonable assurance that the Company’s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of September 24, 2025, and if subservice organization applied the complementary controls assumed in the design of the Company’s controls as of September 24, 2025.

Management of Lockt, LLC
September 24, 2025

Section 3

System Description

System Description

Management's Description of the Lockt Platform
As of September 24, 2025

Types of Services Provided

The Lockt Platform (the Platform) provides cloud-based, physical access control solutions for businesses, schools, healthcare facilities, and other organizations. The Platform is designed to streamline operations by enabling centralized control, automating credential provisioning, and reducing manual processes.

Lockt is responsible for the development and maintenance of the Platform, which is supported entirely by cloud-hosted infrastructure. The Platform is made available to end-users through a web and mobile application and integrates with external systems through a variety of options, including REST API, physical and logical access interoperability (PLAI Agent), LDAP connectors, and file-based transfer methods.

Principal Service Commitments and System Requirements

Management's Description of the Lockt Platform was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

Service Commitments

Service commitments include those made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security objectives and commitments are made available to customers through reseller agreements and information shared on the Company's website. The following summarizes the Company's principal service commitments that management believes to be relevant to the report users:

- The Company uses commercially reasonable physical, managerial, and technical safeguards designed to secure data from accidental loss and unauthorized access.
- Customer data is encrypted at rest and in transit.
- Access to critical resources and sensitive information requires multi-factor authentication and is provided based on the principle of least privilege.
- The Company continuously monitors access to its infrastructure.

System Requirements

The Company's system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop services provided.

Components of the System

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle, such as initiation, authorization, processing, recording, and reporting for the services provided to user entities. The system boundaries do not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

The components of the Platform can be classified into the following five categories:

Infrastructure: The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.

Software: The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile, desktop, or laptop applications.

People: The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

Data: The types of data used by the system, such as transaction streams, files, databases, tables, and other outputs used or processed by the system.

Procedures: The automated and manual procedures related to the services provided, including procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

The Company leverages the experience and resources of IONOS Cloud to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Platform architecture within the cloud hosting environment to ensure security and resiliency requirements are met.

The specific services utilized to support the Platform's cloud infrastructure include the following:

Cloud Hosting Services	
Service	**Description**
Redis	Key-value database service used for rate-limiting
Memcache	In-memory database used for session management
IONOS Virtual Machines	Compute service
IONOS Backup	Centrally managed and automated backup service
IONOS Cloud Firewalls	Filter unwanted traffic upstream and in front of server infrastructure
IONOS Virtual Private Network	Provides a logically isolated virtual network that uses network security groups to control traffic
Microsoft SQL Server	Installed and maintained by the Company within IONOS cloud infrastructure with synchronization and mirroring configured using Redgate software managed by the Company

Software

Software consists of the programs and software that support the Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Platform includes the following:

Software Summary	
Application	**Purpose**
Drata	Compliance management platform
Microsoft 365	Email, file sharing, messaging (Microsoft Teams), and other tools
GitLab	Code repository and CI/CD
Microsoft Entra ID	Identity and authentication
Jira	Project management and issue tracking
Slack	Communication hub
Semgrep	Static code scanning and analysis
CloudAccess API	Application monitoring and audit logs

Software Summary	
Application	**Purpose**
Avast One	Endpoint security
Bitwarden	Password manager
OWASP ZAP	Web application vulnerability scanning

Critical Tools and Resources

The Information Security Program and scope of the system description applies to all infrastructure and software identified in the previous sections. Control activities and procedures are applied to internal systems using a risk-based approach that primarily considers the sensitivity of information stored or processed by the system and its role in maintaining the security of the Company's information. The systems deemed by management vital to meeting its service commitments and system requirements are defined as "Critical Tools and Resources" throughout this description. They include the following:

- IONOS Cloud
- GitLab
- Bitwarden
- Microsoft 365
- Microsoft Entra ID

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. The table below summarizes the key roles and functional responsibilities of the Company. Due to the Company's size, one individual may serve multiple roles.

Organizational Structure	
Role	**Function**
Investors	Responsible for oversight of the development and implementation of internal control and includes members independent of management
President	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities in addition to the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Executive Management	Cross-functional team responsible for oversight, implementation, and continual improvement of the Information Security Program
Business Operations	Manages internal business needs such as human resources, customer success, and other administrative functions
Engineering	Responsible for the development, testing, deployment, and maintenance of the Platform and for maintaining security

The Company leverages a remote workforce for the Platform's management, operation, and security with individuals worldwide. Certain individuals within the Company's core team may be hired legally as independent contractors but are subject to identical controls as individuals hired as "employees" within the context of this system description; thus, both classes are defined as "personnel" throughout the report.

The Company may also work with other individuals hired for a specific project or a defined period. The Company performs a risk assessment for these individuals, as defined in the vendor management process. Controls are implemented based on risk factors, such as level of access and responsibility for sensitive information. These individuals are described as "contractors" within the remaining scope of this description.

Procedures

Procedures are the specific actions undertaken to implement a process, consisting of linked procedures designed to accomplish a particular goal. Policies, which serve as the basis of procedures, are management's statements of what should be done to meet system objectives and may be documented, explicitly stated in communications, or implied through actions and decisions. The Company has adopted the following defined set of information security standards and policies (described as the Information Security Program throughout the report):

- Acceptable Use Policy
- Backup Policy
- Code of Conduct
- Data Protection Policy
- Encryption Policy
- Information Security Policy
- Physical Security Policy
- Risk Assessment Policy
- System Access Control Policy
- Vulnerability Management Policy
- Logging and Monitoring Policy
- Asset Management Policy
- Business Continuity Plan
- Data Classification Policy
- Disaster Recovery Plan
- Incident Response Plan
- Password Policy
- Responsible Disclosure Policy
- Software Development Lifecycle Policy
- Vendor Management Policy
- Data Retention Policy
- Change Management Policy

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners.

The following table details the types of data collected by the Company in connection with the Platform's services and the infrastructure, software, and third-party vendors utilized to store and process the data.

Data Type Summary		
Type	**Description**	**Storage and Processing**
Account data	Personally Identifiable Information and other administrative data from personnel, customers, and other third parties	IONOS Cloud and other third-party managed applications
Access device and event data	Physical access event data captured via integrated devices and equipment issued to end users	IONOS Cloud
Access management data	Access rules, roles, and credentials stored and processed on behalf of users	IONOS Cloud
Secrets	Internal access credentials, tokens, certificates, API keys, and other secrets	Bitwarden, IONOS Managed Redis
Log information	Information relevant to and explicitly necessary for services, including metadata	CloudAccess API, Microsoft SQL Server

System Incidents

There were no identified significant system incidents that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements as of September 24, 2025.

Applicable Trust Services Criteria and Related Controls

The trust services criteria are classified into five categories: security, availability, processing integrity, confidentiality, and privacy. Depending on which category or categories are included within the scope of the description, the applicable trust services criteria consist of criteria common to all five of the trust services criteria (common criteria) and additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories. The common criteria constitute the complete set of criteria for the security category.

The trust services category or categories in scope for this report are as follows:

> **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the confidentiality of information or systems and affect the entity's ability to meet its objectives.

The common criteria are organized as follows:

Control Environment: Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

Communication and Information: Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.

Risk Assessment: The entity's identification and analysis of relevant risks to achieving its objectives, forming a basis for determining how the risks can be managed.

Monitoring Activities: The criteria relevant to how the entity monitors the system, including the suitability of design and operating effectiveness of controls, and acts to address deficiencies identified.

Control Activities: The policies and procedures that help make sure management's directives are carried out.

Logical and Physical Access Controls: The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.

System Operations: The criteria relevant to how the entity manages the operation of systems and detects and mitigates processing deviations, including logical and physical security deviations.

Change Management: The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.

Risk Mitigation: The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Control Environment

The Company's control environment describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. A control environment is the foundation on which an effective system of internal control is built and operated in an organization that strives to achieve its strategic objectives, provide reliable reporting to internal and external stakeholders, operate its business efficiently and effectively, comply with all applicable laws and regulations, and safeguard its assets.

Integrity and Ethical Values

Integrity and ethical behavior are the products of the Company's ethical and behavioral standards, communicated, monitored, and enforced in its business activities. The Company's standards of conduct outline its commitments to integrity and ethical values are made available to all personnel. These commitments include management's actions to remove or reduce incentives, pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts.

Oversight Responsibility

The Company has determined that an independent board of directors is not necessary at this time. The size and complexity of the organization allow the President to provide personal oversight of organizational structure operations, the ability to affect ethical values, and the ability to attract, retain, and hold personnel accountable. The President actively participates in the operation of key controls (by exercising a high level of supervision and review) to provide adequate internal control oversight and mitigate risks. The Company has additional oversight provided by Investors, independent of management. The President is in regular contact with Investors and provides an informal update each quarter to summarize objectives and key results.

Organizational Structure, Authority, and Responsibility

The Company's organizational structure provides the framework within which its activities for achieving objectives are planned, executed, and monitored. A formal organizational chart is in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel. Management established the operating structure based on its size and the nature of its control environment and designed reporting lines to establish key areas of authority and the proper flow of information. Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program. Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.

Commitment to Competence

Management demonstrates its commitment to competence through established policies and practices that attract, develop, and retain sufficient and competent individuals to support the achievement of objectives. The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year. The primary objective of the security training program is to educate personnel on their responsibility to protect the confidentiality, availability, and integrity of the Company's information.

Management has established formal and informal procedures that consider the background and technical competency of potential and existing personnel and vendors when determining whether to hire or retain the individual. Prospective hiring candidates are subject to a formal interview process, reference checks, and/or formal background checks prior to onboarding, with procedures performed that are proportional to legal requirements, business needs, and perceived risks.

Accountability

The Company expects individuals to be held accountable for their internal control responsibilities in pursuing objectives. Management establishes performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct and considering the achievement of both short-term and long-term objectives. Individual performance is evaluated through periodic one-on-one sessions and regular feedback provided informally.

External Individuals

The Company's commitment to integrity and ethical values extends to its use of contractors and vendors. Management considers the use of service providers, who may impact security, confidentiality, and privacy in its processes to establish conduct standards, evaluate adherence to those standards, and promptly address deviations. Information security requirements for mitigating the risks associated with a supplier's access to the Company's assets are formalized with the supplier and documented.

Service providers, such as contractors, who may impact the security of the production environment or have access to customer data, are required to read and accept a non-disclosure agreement. As a general practice, the Company leverages the services of vendors generally accepted in the industry and typically shares their commitments towards security, confidentiality, and privacy available to the public, which is reviewed by personnel to ensure consistency with the Company's policies.

Outsourced Software Development Services

The Company utilizes a third-party development agency (Cube One) to provide front-end, back-end, and DevOps software development services, which are subject to the Company's Vendor Management Policy. Management has assessed and manages the risks associated with the development services provided through the implementation of controls. The scope of services provided has been defined in a written contract and performed under the direct supervision of the Company's personnel. Cube One's employees have access to GitLab and other systems, and privileges are limited to the minimum access necessary to perform the services and any application development changes require a formal code review process.

Communication and Information

A critical objective for the Company is ensuring relevant and quality information is obtained or generated to support the functioning of internal control. The Company has established processes to identify information requirements and ensure appropriate internal and external sources of information are properly captured to support the functioning of other internal control components. Network architecture diagrams have been prepared, and are shared with authorized individuals to communicate information about system operation and boundaries.

Internal Communication

The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel. Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually. Management also reinforces the Information Security Program in meetings, internal communication, and during annual security training and awareness programs.

Management has established specific communication channels to ensure personnel have the necessary information to understand and carry out their internal control responsibilities. Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all-hands meetings are held frequently to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the all-hands meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. The Company considers the timing, audience, and nature of the information when selecting the appropriate communication medium, allowing management to communicate changes to control objectives in a timely manner.

The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls. Formal procedures are established and documented in the Company's plans for incident response that describe how to report system failures, incidents, concerns, and other complaints to appropriate personnel.

External Communication

The Company has prioritized maintaining open communication channels with external parties that allow input from customers, business partners, external auditors, and others to provide management with relevant information. The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.
Agreements are established with critical vendors and business partners that clearly define terms, conditions, and responsibilities. Security objectives and commitments are made available to customers through reseller agreements and information shared on the Company's website.

The Company makes information available about the design and operation of the Platform and its boundaries to users through the customer onboarding process and other technical support. Customers and other external users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.

Product updates are shared with customers so the Company can continue to innovate and maintain the security of the Platform. Multiple marketing channels are available to share new features, and the Company selects the appropriate method, frequency, and messaging based on the specific feature being shared. The Company maintains a public changelog, made available on its website, to communicate product releases, bug fixes, and enhancements. Significant changes, such as those that require action by the user to maintain functionality or impact security requirements, are communicated to users directly and in advance of the implementation.

Risk Assessment

The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks. The first step of the risk assessment process is to identify assets within the scope of the Information Security Program. The objectives identified by management are specified in the risk management program to enable the identification and assessment of risk related to the objectives.

The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to assets and service commitments are identified, and the risks are formally assessed. The Company's fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from IT and access to information.

Risk management discussions include a consideration of how changes in the environment impact risk, such as revisions to the Company's business model, personnel turnover, and the implementation of new systems and technology, which may create new risks that could significantly impact the Company's ability to meet its objectives. Executive Management meets weekly to prioritize and monitor mitigation strategies so the team can react to emerging risks.

Monitoring Activities

The Company selects, develops, and performs ongoing and, if necessary, separate evaluations to ascertain whether the components of internal control are present and functioning. Management considers the rate of change in business and business processes when selecting and developing separate ongoing evaluations and utilizes the current state of the internal controls to establish a baseline.

The following describes the primary methods currently utilized by management:

> **Penetration Testing:** The Company engages third parties to conduct penetration tests of the production environment at least annually. The penetration tests are performed by a certified penetration tester to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Management reviews the results, and high-priority findings are tracked to resolution.
>
> **Code Scanning:** The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Testing is performed against all open pull requests and every 24-hours across the production code with rules established to identify OWASP vulnerabilities, unmasked secrets, and other potential threats. Alerts are communicated to Slack and remediated according to the assessed risk.

Security Testing: The Company performs dynamic application security testing utilizing OWASP ZAP, which is initiated based on the risk level of a particular build and performed at least annually. Vulnerabilities identified are reviewed by management, prioritized, and remediated according to risk significance.

Threat Detection: The Company utilizes Avast One to centralize threat collection, detection, response, and investigation efforts. This service collects data across multiple components of the Platform's surface area and provides threat intelligence and security analysis capabilities that facilitate threat visibility, alert detection, threat response, and proactive hunting. Alerts are configured to notify management of unusual activity and are promptly reviewed for potential impact on the Platform.

Monitoring of Cloud Environment: The Company evaluates risks related to IONOS Cloud and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary. Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel. Production systems are configured to monitor, log, and self-repair or alert on suspicious changes to critical system files and unauthorized intrusions and access attempts.

Access Logs: The Company maintains user access logs for privileged access and for access to user data, which are periodically reviewed by the President. Logical access to audit logs is restricted to authorized personnel, and system administrators are not permitted to erase or deactivate logs of their own activities.

The results of ongoing and separate evaluations are provided to the appropriate individuals to assess results. The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action, and provide visibility to senior leaders regarding the timeliness of remediation.

Control Activities

Control activities are the actions established through policies and procedures that help ensure management's directives to mitigate risks to achieve objectives are carried out. They may be preventative or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations, and business performance reviews.

Compliance Management Platform

Management leverages a compliance management platform (Drata) to support the design, implementation, operation, monitoring, and documentation of its control activities. The platform captures data via APIs across multiple technology providers, including identity providers, infrastructure providers, version control systems, ticketing systems, and human resource information systems, to provide a central dashboard for compliance activities.

Drata is also utilized to support the following:

- Continuous automated monitoring of certain security controls
- Compliance checks on personnel workstations
- Inventory management
- Communication and documentation of review, approval, and acknowledgment of information security policies
- Real-time visibility to manage the Information Security Program

Use of a compliance management platform does not relieve management of its responsibilities for designing, implementing, and operating the Information Security Program. Management is also responsible for evaluating the accuracy and completeness of the information produced, maintained, and aggregated by Drata, which is performed through an annual risk assessment and necessary due diligence procedures, such as obtaining and reviewing the platform's most recent SOC 2 Type 2 report.

Information Security Program Development and Maintenance

As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. The risk assessment process includes the selection and development of control activities over technology infrastructure, designed and implemented to help ensure the completeness, accuracy, and availability of technology processing. Specifically, management selects and develops control activities designed and implemented to restrict technology access rights and achieve management’s objectives over the acquisition, development, and maintenance of technology and infrastructure.

The Information Security Program is reviewed by management annually and formally approved. The Company’s policies and procedures are designed to govern an individual’s day-to-day activities and establish expectations and relevant procedures specifying actions. Management assigns competent personnel with sufficient authority the responsibility to promptly perform control activities and duties with diligence and continuing focus.

Logical and Physical Access Controls

The Company has established policies and procedures that define the access control requirements for requesting and provisioning user access to the system. Duties and access to sensitive resources are established based on the principle of least privilege. Logical access to systems is restricted through access control software and rule sets and is controlled by limited administrative users. Individuals require a unique username and are identified and authenticated before accessing information assets. Access to Critical Tools and Resources requires multi-factor authentication.

The Company has established a formal onboarding and termination process. Appropriate management approval is obtained before granting access to Critical Tools and Resources. The Company’s compliance management platform performs automated checks and triggers alerts if users access certain resources without appropriate approval and completion of the onboarding process.

The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels. Accounts for personnel who have been terminated or no longer require access are disabled within one business day.

Privileged access to Critical Tools and Resources is highly restricted. Users with multiple access levels (e.g., administrators) are given separate accounts for normal system use and administrative functions. The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection. Access to migrate changes to production is restricted to authorized individuals with a business need.

Full-disk encryption is implemented for all personnel workstations and laptops. Personnel accessing Critical Tools and Resources utilize laptops with the most recent operating system security updates and configured with antivirus software.

Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company. Information and data assets are subject to the Company's policies and procedures for data protection, classification, and retention, which define parameters for the ownership, classification, security, storage, and retention of data. Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.

The Company's policies and procedures define the requirements for proper and effective use of cryptography to protect information confidentiality, authenticity, and integrity. Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks. Encryption is used to protect customer data at rest. Customer data is encrypted when stored in database tables, temporary files, and backups using 256-bit Advanced Encryption Standard.

Points of access by outside entities and the types of data that flow through the access points are identified, inventoried, and managed. The Company uses firewalls and configures them to protect against threats from sources outside the boundaries of the system. Management performs a review of its firewall rules on an annual basis.

System Operations

The Company has established baseline configuration standards and uses tools to detect and restore configuration deviations from the standards. Infrastructure is monitored for noncompliance with the configuration standards, which could threaten the achievement of the Company's objectives. The infrastructure is built upon standard machine images that have been obtained from trusted sources. Identified security deficiencies are tracked and prioritized through internal tools according to their severity.

Applicable security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Processes are in place to evaluate patches and their applicability to the environment. Once the patches have been reviewed and their criticality level is determined, service teams determine the patch implementation strategy.

Formal procedures are defined for security event detection and management, including the provision of resources. The Company uses a system that collects and stores logs in a central location. The system can be queried in an ad hoc fashion by authorized users. Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.

The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents. Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence. Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals. Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned. The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.

Change Management

The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems. The change management processes and procedures have been established to plan, schedule, apply, distribute, and track changes to the production environment to minimize risk and client impact.

The Company uses a version control system to manage source code, documentation, release labeling, and other change management tasks. Software developers are expected to adhere to the Company’s coding standards throughout the development cycle, including standards for quality, commenting, and security. Releases are tested throughout the development process and validated prior to deployment. Testing is performed in an isolated environment that is separate from production workloads.

Code changes include a formal code review process. Only experienced and knowledgeable engineers with experience in code review techniques and secure coding practices can approve a code change. Overrides of edit checks, approvals, and changes to confirmed transactions are appropriately authorized, documented, and reviewed. Changes to the production environment are announced in Slack and Microsoft Teams prior to initiating the deployment. Changes requiring downtime are also posted to the Company's status page via maintenance alert.

Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the Company's commitments and system requirements. Upon the identification of a deficiency, processes are in place for authorizing, designing, testing, approving, and implementing changes necessary in the event a change needs to be implemented in an urgent timeframe.

Risk Mitigation

The Company implements risk mitigation strategies to prioritize, evaluate, and implement the appropriate risk-reducing controls recommended by the risk management process. The Company's plans for business continuity, disaster recovery, and incident response are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from security events and incidents. Cybersecurity insurance is maintained to mitigate the financial impact of business disruptions.

As part of its risk mitigation strategies, management assesses and manages risks associated with vendors and business partners. Periodically, generally annually, but performed relative to risk and changes in the environment, management assesses the risks that vendors and business partners represent to the achievement of the Company's objectives. As a general practice, the Company utilizes software and infrastructure resources and applications that are industry leaders and generally accepted amongst the security community.

The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided and other factors, and a review of the vendor's security, confidentiality, and privacy requirements. Based on the risk assessment, management obtains due diligence and compliance information, such as SOC 2 Type 2 reports, requested and reviewed during the vendor acceptance and re-review process. The Company has written agreements in place with vendors and business partners that include confidentiality and privacy commitments consistent with the commitments and requirements of the Company.

User Entity Controls and Responsibilities

The Company's services are designed utilizing a shared responsibility model where maintaining the security of a customer's information is dependent upon the customer implementing controls that are outside the Company's control. If these controls are necessary to meet the Company's service commitments and system requirements, they are known as complementary user entity controls (CUECs) as defined by DC 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report*. Other controls that are necessary or recommended for the customer to maintain the security of its information are defined as user entity responsibilities.

Complementary User Entity Controls

The Company has restricted its service commitments to matters for which it is responsible and that can be reasonably achieved by itself, and the Platform's system requirements are derived from those commitments. Therefore, CUECs are not required or significant to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

The Company communicates the expectations or requirements of its users through legal agreements and instructional material, such as user manuals, which are necessary to allow the customer to benefit from the use of the Platform. User entity responsibilities are generally either explicitly required or communicated as a recommended best practice, and the controls presented below should not be regarded as a comprehensive list of controls that user entities should implement.

User entity responsibilities that should be implemented to allow the customer to benefit from the use of the Platform include the following:

- Ensuring the confidentiality of user accounts and passwords
- Notifying the Company promptly when changes are made to technical, billing, or administrative contact information
- Developing internal disaster recovery and business continuity plans that address the inability to access or utilize the Company's services
- Notifying the Company and providing accurate information regarding new, terminated, and changes necessary to user accounts
- Informing the Company of any regulatory issues that may affect the services provided
- Understanding and complying with contractual obligations to the Company
- Immediately notifying the Company of any actual or suspected information security breaches involving the Platform, including compromised user accounts
- Granting access only to authorized and trained personnel
- Deploying physical security and environmental controls for all devices and access points

Subservice Organization Controls

When controls at a vendor are necessary in combination with the Company's controls to provide reasonable assurance that the Company's service commitments and system requirements are achieved, based on the applicable trust services criteria, the vendor is considered a subservice organization. Complementary subservice organization controls (CSOCs) are controls that the Company's management assumed, in the design of the system, would be implemented by subservice organizations and are necessary, in combination with controls at the Company, to provide reasonable assurance that the Company's service commitments and system requirements were achieved. Management has identified the below subservice organization and has elected to use the carve-out method for the purposes of this report:

Complementary Subservice Organization	
Subservice Organization	**Description**
IONOS Cloud	Cloud hosting services

The Company has implemented procedures for the oversight and monitoring of the services provided by the subservice organization, which are outlined in the vendor management policies and procedures. Personnel are highly trained to manage the cloud infrastructure and regularly review technical resources made available through technical training and industry forums to understand key concepts and implement controls necessary to meet the Company's responsibilities described in the shared responsibility model for each specific service utilized. Management also reviews available compliance reports and monitors the subservice organization through regular communication and interaction with the environment.

The following are the applicable trust services criteria and controls that are necessary to be in place at the subservice organization to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

Complementary Subservice Organization Controls	
Criteria	**Control**
Logical and Physical Access CC6 Series	Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts and procedures are implemented to decommission and physically destroy production assets securely. Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by the Company, to secure the transmission and storage of information.

Complementary Subservice Organization Controls	
Criteria	**Control**
System Operations CC7 Series	Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities. Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.
Change Management CC8 Series	Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.

Trust Services Criteria Relevance

All security trust services criteria as set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* were relevant to the Platform as presented in this report.

Significant Changes to the System

There have been no changes that are likely to affect report users' understanding of how the Platform is used to provide services as of September 24, 2025.

Use of Report

The description does not omit or distort information relevant to the Platform while acknowledging the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each user may consider important to their own particular needs.

Section 4

Information Provided by Service Auditor

Information Provided by Service Auditor

Engagement Objectives and Scope

A SOC 2 report is intended to provide users of the Lockt Platform with the information necessary to help assess and address the risks associated with the services provided by the Platform. The report is intended for use by those with sufficient knowledge and understanding of the Platform, its services, and the system used to provide those services, among other matters. Without such knowledge, users are likely to misunderstand the contents of the SOC 2 report. Thus, the Independent Service Auditor's Report of MJD Advisors, LLC (MJD) provided in Section 1 is restricted to specified parties who possess the requisite knowledge.

MJD's responsibility in this report is to perform a SOC 2 examination in accordance with AT-C Section 105, *Concepts Common to All Attestation Engagements*, and AT-C Section 205, *Examination Engagements*. According to those standards, the examination is predicated on the concept that management is responsible for the design, implementation, and operating effectiveness of its controls to provide reasonable assurance the organization's service commitments and system requirements were achieved. Management is also responsible for preparing the System Description in Section 3 and Management's Assertion in Section 2 of this report, including the completeness, accuracy, and method of presentation. MJD's responsibility is to design and perform procedures to obtain sufficient appropriate evidence and express an opinion on the presentation of the description and the design of controls.

Management of Lockt, LLC is responsible for determining the point in time (SOC 2 Type 1) or period of time (SOC 2 Type 2) to be covered by the description of the Platform, its assertion, and, consequently, the service auditor's examination. The frequency and period covered by a SOC 2 report is a business decision of management, determined by the needs of its users, and management determined that a SOC 2 Type 1 report was appropriate in the circumstances. MJD's responsibility is to express an opinion on the description and the suitability of the design of controls, further described in Section 1.

MJD did not perform any procedures regarding the operating effectiveness of controls stated in the description.

Compliance Management Platform

As described in the Control Activities section of the System Description, management leverages a compliance management platform (Drata) to support the design, implementation, operation, monitoring, and documentation of its control activities. Drata is also used by management to enhance the efficiency of the examination by collecting and organizing the Company's documentation in a central repository supported by integrated data connections. Information generated by Drata and made available to MJD as audit evidence is considered information provided by the Company. Management is expected to have evaluated the accuracy and completeness of the information produced and maintained.

The responsibility of MJD to obtain sufficient appropriate evidence to support the Independent Service Auditor's Report is unchanged by management's use of Drata. MJD performed certain procedures to determine whether Drata functioned as intended and whether the information generated by Drata was reliable for MJD purposes. Specifically, MJD reviewed Drata's most recently available SOC 2 Type 2 Report.

Control Matrix for the Lockt Platform

The control matrix provides report users with the specific controls management has identified to meet the applicable trust services criteria.

Control Environment

CC1.1: The entity demonstrates a commitment to integrity and ethical values.
Description of the Company's controls
The Company's standards of conduct outline its commitments to integrity and ethical values are made available to all personnel.
Prospective hiring candidates are subject to a formal interview process, reference checks, and/or formal background checks prior to onboarding, with procedures performed that are proportional to legal requirements, business needs, and perceived risks.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.

CC1.2: The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
Description of the Company's controls
The President actively participates in the operation of key controls (by exercising a high level of supervision and review) to provide adequate oversight of internal control and mitigate risks.
The President is in regular contact with Investors and provides an update each quarter that includes a summary of objectives and key results.

Control Environment

CC1.3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in pursuing objectives.
Description of the Company's controls
A formal organizational chart is in place to communicate key areas of authority, responsibility, and applicable lines of reporting to personnel.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program.
Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.

CC1.4: The entity demonstrates a commitment to attracting, developing, and retaining competent individuals in alignment with objectives.
Description of the Company's controls
Job requirements and responsibilities are documented and communicated in formal job descriptions for new positions.
The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year.
Prospective hiring candidates are subject to a formal interview process, reference checks, and/or formal background checks prior to onboarding, with procedures performed that are proportional to legal requirements, business needs, and perceived risks.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.

Control Environment

CC1.5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Description of the Company's controls
The Company's standards of conduct outline its commitments to integrity and ethical values are made available to all personnel.
Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Program.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.

Communication and Information

CC2.1: The entity obtains or generates and uses relevant, quality information to support the functioning of internal controls.
Description of the Company's controls
Network architecture diagrams have been prepared, and are shared with authorized individuals to communicate information about system operation and boundaries.
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.

CC2.2: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
Description of the Company's controls
The Company has implemented a security training program that is required to be completed for all personnel upon hire and renewed each year.
Network architecture diagrams have been prepared, and are shared with authorized individuals to communicate information about system operation and boundaries.
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel.
Personnel are required to review and acknowledge the Information Security Program and standards of conduct upon hire and re-certify their acknowledgment annually.
The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls.
Formal procedures are established and documented in the Company's plans for incident response that describe how to report system failures, incidents, concerns, and other complaints to appropriate personnel.

Communication and Information

CC2.3: The entity communicates with external parties regarding matters affecting the functioning of the internal control system.
Description of the Company's controls
Security objectives and commitments are made available to customers through reseller agreements and information shared on the Company's website.
The Company makes information available about the design and operation of the Platform and its boundaries to users through the customer onboarding process and other technical support.
Customers and other external users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.
The Company maintains a public changelog, made available on its website, to communicate product releases, bug fixes, and enhancements.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.

Risk Assessment

CC3.1: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
Description of the Company's controls
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.
The objectives identified by management are specified in the risk management program to enable the identification and assessment of risk related to the objectives.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

CC3.2: The entity identifies risks to achieve its objectives across the entity and analyzes risks to determine how they should be managed.
Description of the Company's controls
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
Executive Management meets weekly to prioritize and monitor mitigation strategies so the team can react to emerging risks.

Risk Assessment

CC3.3: The entity considers the potential for fraud in assessing risks to achieve objectives.
Description of the Company's controls
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
The Company's fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from IT and access to information.

CC3.4: The entity identifies and assesses changes that could significantly impact the system of internal control.
Description of the Company's controls
The Company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to objectives and service commitments are identified, and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
Executive Management meets weekly to prioritize and monitor mitigation strategies so the team can react to emerging risks.

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.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
The Company evaluates risks related to IONOS Cloud and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.

CC4.2: The entity evaluates and communicates internal control deficiencies promptly to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
The Company evaluates risks related to IONOS Cloud and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary.
The Company uses internal tools to aggregate and monitor identified deficiencies, alert the individuals responsible for corrective action, and provide visibility to senior leaders regarding the timeliness of remediation.

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.
Description of the Company's controls
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.
As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
The Information Security Program is reviewed by management annually and formally approved.
Duties and access to sensitive resources are established based on the principle of least privilege.

CC5.2: The entity also selects and develops general control activities over technology to support the achievement of objectives.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
The Information Security Program is reviewed by management annually and formally approved.
Duties and access to sensitive resources are established based on the principle of least privilege.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.

Control Activities

CC5.3: The entity deploys control activities through policies that establish expectations and procedures that implement policies.
Description of the Company's controls
The Company has a defined Information Security Program that describes policies and procedures to guide personnel in achieving the Company's security commitments and associated system requirements, and is made available to all personnel.
The Information Security Program identifies personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring system controls.
Security objectives and commitments are made available to customers through reseller agreements and information shared on the Company's website.
The Company has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks.
The Information Security Program is reviewed by management annually and formally approved.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.

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.
Description of the Company's controls
Duties and access to sensitive resources are established based on the principle of least privilege.
Access to Critical Tools and Resources requires multi-factor authentication.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.
The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection.
Access to migrate changes to production is restricted to authorized individuals with a business need.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.
Encryption is used to protect customer data at rest.
The infrastructure is built upon standard machine images that have been obtained from trusted sources.

CC6.2: Before 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 users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
Description of the Company's controls
Duties and access to sensitive resources are established based on the principle of least privilege.
Appropriate management approval is obtained before granting access to Critical Tools and Resources.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.

Logical and Physical Access Controls

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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.
Description of the Company's controls
Duties and access to sensitive resources are established based on the principle of least privilege.
Individuals require a unique username and are identified and authenticated before accessing information assets.
Appropriate management approval is obtained before granting access to Critical Tools and Resources.
The Company continuously monitors access to Critical Tools and Resources with its compliance management platform and other periodic checks of access levels.
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
The physical security of the Company's primary resources has been outsourced through a cloud-hosting model, and these controls are carved out for the purposes of this report. See Subservice Organizations described within Section 3.

Logical and Physical Access Controls

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.
Description of the Company's controls
Accounts for personnel who have been terminated or no longer require access are disabled within one business day.
Management maintains a detailed inventory of all information systems that includes classification and prioritization based on the asset's business value and criticality to the Company.
Formal data retention and disposal procedures are in place to guide the secure retention and disposal of Company and customer data.

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
Description of the Company's controls
The Company utilizes Avast One to centralize threat collection, detection, response, and investigation efforts. Alerts are configured to notify management of unusual activity and are promptly reviewed for potential impact to the Platform.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.
Access to Critical Tools and Resources requires multi-factor authentication.
The Company's production systems can only be accessed by authorized personnel via an approved encrypted connection.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
The infrastructure is built upon standard machine images that have been obtained from trusted sources.

Logical and Physical Access Controls

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.
Description of the Company's controls
Full-disk encryption is implemented for all personnel workstations and laptops.
Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
Encryption is used to protect customer data at rest.
The Company uses firewalls and configures them to protect against threats from sources outside the boundaries of the system.
Management performs a review of its firewall rules on an annual basis.
The infrastructure is built upon standard machine images that have been obtained from trusted sources.

Logical and Physical Access Controls

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.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
Logs are aggregated centrally and monitored for indicators of compromise. Alerts are generated based on thresholds established to define potential suspicious activity and are reviewed by the appropriate personnel.
Duties and access to sensitive resources are established based on the principle of least privilege.
Personnel accessing Critical Tools and Resources utilize laptops with the most recent operating system security updates and configured with antivirus software.
The infrastructure is built upon standard machine images that have been obtained from trusted sources.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.

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.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
The infrastructure is built upon standard machine images that have been obtained from trusted sources.
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.

System Operations

CC7.2: The entity monitors system components and the operation of those components for anomalies 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.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
The Company utilizes Avast One to centralize threat collection, detection, response, and investigation efforts. Alerts are configured to notify management of unusual activity and are promptly reviewed for potential impact to the Platform.
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.

System Operations

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.
Description of the Company's controls
The Company engages third parties to conduct penetration tests of the production environment at least annually. Management reviews the results, and high-priority findings are tracked to resolution.
The Company utilizes Semgrep to perform Static Application Security Testing (SAST) of the Platform's source code for vulnerabilities. Alerts are communicated to Slack and remediated according to the assessed risk.
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.
The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.
Appropriate communication channels have been established to share the necessary information regarding security events with management, users, and other key individuals.

System Operations

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.
Description of the Company's controls
Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events. Personnel are assigned to configure the monitoring tools, and the appropriate individuals receive real-time alerts through the generation of emails and other messaging tools.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.
The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.

System Operations

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.
Description of the Company's controls
Identified security deficiencies are tracked and prioritized through internal tools according to their severity.
The Company has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents.
Security events are quantified, monitored, and tracked by an identified incident response team, and procedures identified include collecting and preserving information that can serve as evidence.
Post-mortem meetings are conducted for security incidents to discuss the root causes, remediation steps, and lessons learned.
The Company's plans for incident response require creating, prioritizing, assigning, and tracking follow-ups to completion.

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.
Description of the Company's controls
The Company maintains a public changelog, made available on its website, to communicate product releases, bug fixes, and enhancements.
Duties and access to sensitive resources are established based on the principle of least privilege.
Access to migrate changes to production is restricted to authorized individuals with a business need.
The Company has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems.
The Company uses a version control system to manage source code, documentation, release labeling, and other change management tasks.
Releases are tested throughout the development process and validated prior to deployment.
Testing is performed in an isolated environment that is separate from production workloads.
Changes to the production environment are announced in Slack and Microsoft Teams prior to initiating the deployment.
Code changes include a formal code review process. Only experienced and knowledgeable engineers with experience in code review techniques and secure coding practices can approve a code change.

Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
Description of the Company's controls
The Company's plans for business continuity, disaster recovery, and incident response are documented and made available to Company personnel to provide guidance for detecting, responding to, and recovering from security events and incidents.
Cybersecurity insurance is maintained to mitigate the financial impact of business disruptions.

CC9.2: The entity assesses and manages risks associated with vendors and business partners.
Description of the Company's controls
The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels, criticality to services provided and other factors, and a review of the vendor's security, confidentiality, and privacy requirements.
Vendors and business partners are subject to due diligence procedures that include a review of security, confidentiality, and privacy commitments provided through terms of service and written agreements to ensure consistency with the commitments and requirements of the Company.

End of Report