LabVantage Security Addendum

Table of Contents

LabVantage Security Addendum

Executive Summary
We recognize that our customers entrust us with critical business processes and sensitive data. Our Information Security Management System (ISMS), and privacy program, are designed to meet or exceed ISO/IEC 27001 and AICPA SOC 2 (Trust Services Criteria). This document outlines LabVantage's governance, risk management, technical and organizational controls, and audit posture to protect customer data.,

SOC 2 Type 2 Evaluation (Security Operational Controls)
LabVantage is assessed against SOC 2 by a third-party evaluation company (performed by an AICPA-qualified auditor) and undergoes annual SOC 2 Type 2 audits. During the audit our procedures are reviewed, and operational objective evidence is provided to prove that we follow our procedures, for compliance with the 154 SOC 2 security and privacy controls, as listed below. The SOC 2 Type 2 report can be provided upon request and an executed NDA.

ISO 27001:2022 Certification
LabVantage has been certified to ISO 27001 since 2019 and undergoes an annual compliance audit and a full recertification audit every 3 years by an accredited third-party certifying company. During the audit our procedures are reviewed, and operational objective evidence is provided to prove that we follow our procedures, for our compliance to the 93 ISO 27001 security and privacy controls. The procedures include, but not limited to, Acceptable Use, Access Control, Secure Development, Change Management, Vulnerability Management, Incident Response, Business Continuity, and Vendor Risk. The Statement of Applicability has the full list of controls and procedures, and the ISO 27001 audit report can be provided upon request and an executed NDA.

CyberVadis Assessment
On an annual basis, our security and data protection / privacy processes are evaluated by CyberVadis. A CyberVadis assessment is a third-party risk assessment process that evaluates cybersecurity maturity through an evidence-based methodology. It combines automated questionnaires with analyst validation to assess a supplier's security policies, practices, and infrastructure, providing a detailed score and report. The goal is to give visibility into the cybersecurity posture, identify risks, and help improve security.

1) **Governance**
   - Our Information Security Management System (ISMS) is aligned to the SOC 2 Trust Services Criteria for Security, Availability, and Confidentiality and to ISO 27001:2022, covering policy framework, risk management, leadership commitment, and continuous improvement.
   - A formal risk methodology (likelihood / impact scoring) is in place with annual assessments, risk treatment plans, and residual risk acceptance by executive leadership. Risk register items are tracked to closure with measurable controls.
   - A designated Information Security Management function oversees security strategy, supported by Quality, Information Technology. Legal, and other departments. A cross-functional ISMS Steering Committee reviews risks, KPIs, and control effectiveness.
   - Mandatory security and privacy training during onboarding and annually, with targeted modules for engineers (secure coding, threat modeling) and operations (incident management, BCP/DR).
   - Documented security policies, standards, and procedures are maintained, version-controlled, communicated, and reviewed at least annually.
2) **Risk Management**
   - Asset and scenario based formal risk management process with annual evaluations and management approvals, to identify operational, data center, and AI risks, threats, and controls to mitigate the risks.
3) **Asset and Configuration Management**
   - All in-scope assets (endpoints, servers, applications, cloud resources, network components, etc.) are inventoried, classified by sensitivity, and assigned ownership.

- Hardened secure baseline configurations are documented, enforced and monitored for drift.
- Software, system, and infrastructure changes follow a change control process with documented approvals, testing, segregation of duties, and rollback plans.

4) Identity, Access, and Authentication

- Role-Based Access Control (RBAC) with least privilege and need to know, with separation of duties between departments (development, testing and others) and privileged access management for admin functions.
- Unique user authentication using SSO and MFA enforced for all workforce users.
- Joiner / Mover / Leaver processes grant, modify, and revoke access within one business day of status change.
- Administrative and console access to production and cloud control planes require MFA and all privileged and non-privileged sessions are monitored and logged.
- Strong credential policies (unique user IDs, salted hashing, password complexity and rotation, shared accounts are forbidden).
- Password requirements include: a minimum length of eight (8) characters with three of the four following requirements: 1) upper case letter, 2) lower case letter, 3) number, and 4) special character. Passwords automatically expire every 90 days, and previous passwords cannot be used.
- Connections to SaaS environments are only accessible via JumpHost software which allows or denies access, logs the user credentials / date / time, and automatically terminates the connection after a period of time.
- Access to SaaS production environments is restricted to only Cloud Ops and Support personnel.
- Access to SaaS development and test environments are restricted to Cloud Ops, Support and authorized Professional Services employees that are working on the applicable customer's customer's project. Once the project is over, access is revoked.

5) Training and Personnel Security

- All personnel and contractors complete security and privacy training at the time of hire and annually.
- All personnel and contractors are assigned training based on their role and job function.
- Background checks are conducted in accordance with applicable law and role sensitivity; disciplinary processes address policy violations.

6) Privacy and Data Lifecycle

- Purpose limited / restricted collection and processing with appropriate legal bases and support of subject and customer rights.
- Enforced retention schedules with verified deletion provided upon request.

7) Logging, Monitoring, and Detection

- Comprehensive event logging and audit trails with centralized time-synchronization, tamper resistance, access controlled and retention, to capture all activities regardless of the level of permissions or security.
- Logs are reviewed for failures and suspicious activities.

8) Incident Response and Breach Notification

- Documented incident response plan aligned with ISO 27001, SOC 2, GDPR and other data privacy regulations, that defines roles, escalation, documentation, tracking, evidence handling, and communication.
- Annual exercises of security and data breach process.
- Timely notification, without undue delay, of security incidents affecting Customer data or service commitments are reported to the Customer and Supervisory Authority (if needed). Notification includes scope, impact, containment, and remediation actions.
- Post-incident reviews / lessons learned performed with CAPAs tracked to closure.

9) Network Security

- Logical segmentation isolating Customer SaaS environments from other Customer environments and from the LabVantage network.

- Public endpoints are protected by WAF, rate limiting, and DDoS controls; inbound and outbound rules are documented, reviewed at least annually.
- Daily vulnerability scanning (e.g.: WIZ) for vulnerabilities and issues remediated.
- Annual penetration tests are executed by an independent qualified third-party testing company, issues remediated and retesting documented.

10) Data Protection and Cryptography

- Customer data is classified as restricted by default.
- No persistent storage of customer data on employee laptops to reduce the risk of data breach and loss.
- Data is only collected and used for the purpose it is intended for, accessed by only the employees needing to use it, stored for the shortest period and then securely disposed.
- Data Protection Agreements (DPA), Standard Contractual Clauses (SCCs), and Quality Assurance Agreements (QAA) are in place to control data processing as required.
- Minimum of AES-256 (or equivalent) at rest; TLS 1.2+ in transit; key access restricted to only IT and rotated annually or upon compromise.
- Encrypted, access-controlled backups retained ≥14 days; restoration tested annually.

11) Vulnerability and Patch Management

- Daily vulnerability scanning of the infrastructure, LabVantage and Customer SaaS systems.
- Critical vulnerabilities remediated within 3 days; High within 30 days; and Medium within 180 days. A formal risk acceptance assessment, with compensating controls and management approval, will be developed if these timelines cannot be met.
- Third-party libraries monitored.
- Defined system and application patch cadence, with expedited procedures for active threats.

12) Secure Software Development (SSDLC)

- Agile methodology and GAMP 5 deliverables, including validation evidence, are in place for all software versions.
- Automated build process is in place to ensure reproducible builds.
- Developers receive secure development training.
- Secure coding standards are aligned with OWASP, and other known vulnerabilities, and enforce language-specific best practices.
- All software versions are stored in a secure repository with restricted access.
- All code undergoes peer review or automated Static Application Security Testing (SAST) (SonarQube) during coding for any known vulnerabilities.
- Prior to software version release, all software is tested by a third-party vulnerability testing company. All reported critical, all high and, as many as the medium and low vulnerabilities, are remediated and then the software retested for verification.

13) Data Center / Cloud Infrastructure Security

- All systems and SaaS reside on the Amazon Web Services (AWS) platform, which includes security standards and certifications as detailed below.

14) Business Continuity Plan and Disaster Recovery Plan

- BCP addresses personnel, facility, and resource disruption, with various pre-planned scenarios and tested annually with a desktop exercise or actual event.
- DRP defines encrypted backups, retention, RTO/RPO, recovery, and dependencies and is tested annually.
- High-availability architectures and capacity monitoring support committed service levels; failover procedures shall be documented and periodically exercised.

15) Supplier Management

- Risk based supplier management process to evaluate and qualify suppliers for their QMS, ISMS, privacy, contractual security requirements, processes, and operation sustainability.
- Suppliers are rated for risks to the business and data processing and managed in the supplier risk register.

- Suppliers are evaluated on a periodic basis, (high risk suppliers are qualified annually and medium risk suppliers every 2 years) with documented audit reports issued and corrective actions created for remediations.

16) Evidence and Customer Verification

- Upon reasonable notice, and under an executed NDA, documented evidence of our compliance to ISO 27001, SOC 2 Type 2, CyberVadis, and other regulations and processes can be provided.
- Detailed results of penetration and vulnerability testing are not provided for security reasons, but executive summaries can be provided.

17) SOC 2 Controls

Control #	SOC 2 Control Requirements
Control Environment	
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	A documented employee handbook and policy manual are in place to communicate organizational policy statements and codes of conduct.
CC1.1.2	Employees are required to sign an acknowledgment form upon hire indicating they have been given access to the policy manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
CC1.1.3	Employees are required to sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client data, to unauthorized parties.
CC1.1.4	Background checks are performed by a third-party service provider as a component of the hiring process.
CC1.1.5	An employee sanction procedure is in place and documented within the employee manual to communicate disciplinary procedures for noncompliance with associated policies and procedures.
CC1.1.6	Management personnel conduct performance reviews of employees on an annual basis to evaluate employees against expected levels of performance and conduct.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	The executive leadership team exercises oversight of operations and the development and performance of internal control.
CC1.2.2	The executive leadership team meets on an annual basis to measure the development and performance of internal control.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	An organizational chart is in place and made available to employees to define and communicate lines of reporting.
CC1.3.2	The executive leadership team meets on an annual basis to measure the development and performance of internal control.
CC1.3.3	A management review meeting including execute leadership occurs on an annual basis to discuss long-term business goals, results of internal and external audits, and company risks.
CC1.3.4	Documented position descriptions are in place to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	New employee onboarding procedures are in place to guide the onboarding process.
CC1.4.2	Employees are required to sign an acknowledgment form upon hire indicating they have been given access to the policy manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
CC1.4.3	Employees are required to sign a confidentiality statement upon hire agreeing not to disclose proprietary or confidential information, including client data, to unauthorized parties.

LabVantage

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
CC1.4.4	Background checks are performed by a third-party service provider as a component of the hiring process.
CC1.4.5	Documented position descriptions are in place to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
CC1.4.6	An employee sanction procedure is in place and documented within the employee handbook to communicate disciplinary procedures for noncompliance with associated policies and procedures.
CC1.4.7	Management personnel conduct performance reviews of employees on an annual basis to evaluate employees against expected levels of performance and conduct.
CC1.4.8	Employees are required to complete security awareness training upon hire to understand their obligations and responsibilities to comply with the security policies.
CC1.4.8	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC1.4.9	Phishing exercises are completed on at least annual basis to help ensure that employees understand their responsibilities for reporting on potential or actual threats to system security. Employees that fail the exercise are required to take further training.
CC1.4.10	A notification email is sent to all employees on an annual basis that includes information about any changes to the IT policy.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	An employee sanction procedure is in place and documented within the employee manual to communicate disciplinary procedures for noncompliance with associated policies and procedures.
CC1.5.2	An organizational chart is in place and made available to employees to define and communicate lines of reporting.
CC1.5.3	Documented position descriptions are in place to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
CC1.5.4	Management personnel conduct performance reviews of employees on an annual basis to evaluate employees against expected levels of performance and conduct.
Communication and Information	
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	
CC2.1.1	An information security policy is formally documented that identifies the information required to support the functioning of internal control and achievement of objectives.
CC2.1.2	An enterprise monitoring application is utilized to monitor the availability and performance of production servers and network devices.
CC2.1.3	The enterprise monitoring application is configured to send notifications to IT and operations personnel when pre-defined thresholds are exceeded on monitored network devices.
CC2.1.4	An automated vulnerability management application is in place to scan network assets for vulnerabilities on a continuous basis.
CC2.1.5	A SEIM tool is utilized to monitor system events for in-scope systems to identify anomalies within network and system activity and configured to notify the 24X7 third-party Security Operations Center and other security personnel when suspicious network and system activity is identified by the tool.
CC2.1.6	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	An information security policy is formally documented that identifies the information required to support the functioning of internal control and achievement of objectives.

LabVantage

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
CC2.2.2	A SEIM tool is utilized to monitor system events for in-scope systems to identify anomalies within network and system activity and configured to notify the 24X7 third-party Security Operations Center and other security personnel when suspicious network and system activity is identified by the tool.
CC2.2.3	Documented procedures for reporting security incidents are provided to employees to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.
CC2.2.4	An organizational chart is in place and made available to employees to define and communicate lines of reporting.
CC2.2.5	Documented position descriptions are in place to define the expected behavior and skills needed to facilitate the accomplishment of objectives related to the employee's area of responsibility.
CC2.2.6	Employees are required to acknowledge their receipt of the employee manual upon hire as acceptance of their responsibility to adhere to the established policies and procedures.
CC2.2.7	Employees are required to complete security awareness training upon hire to understand their obligations and responsibilities to comply with the security policies.
CC2.2.8	Training courses are available to new and existing employees to maintain and advance the skill level of personnel.
CC2.2.9	Phishing exercises are completed on at least annual basis to help ensure that employees understand their responsibilities for reporting on potential or actual threats to system security. Employees that fail the exercise are required to take further training.
CC2.2.10	Release notes are documented and communicated to employees via the email.
CC2.2.11	A support e-mail is available to internal personnel for reporting of incidents, concerns, and other complaints.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	Information regarding the design, support and operation of the in-scope services is communicated to external users via the company website.
CC2.3.2	The entities commitments and the associated services requirements are documented in customer contracts.
CC2.3.3	A standard service agreement that addresses confidentiality and data protection requirements is required to be in place prior to sharing information designated as confidential with third parties.
CC2.3.4	A support portal is available to external users via the company website to report security incidents, concerns, and complaints.
Risk Assessment	
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	A documented risk management program policy is in place to guide personnel in identifying business objective risks, risks arising from potential business disruptions, assessing changes to the system, and developing risk management strategies as part of the risk assessment process.
CC3.1.2	A management review meeting including execute leadership occurs on an annual basis to discuss long-term business goals, results of internal and external audits, and company risks.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	A documented risk management program policy is in place to guide personnel in identifying business objective risks, risks arising from potential business disruptions, assessing changes to the system, and developing risk management strategies as part of the risk assessment process.
CC3.2.2	A formal risk assessment is performed on an annual basis that considers the impact of achieving business objective risks. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
CC3.3.1	A formal risk assessment is performed on an annual basis that considers the potential for fraud. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	A formal risk assessment is performed on an annual basis that considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process, and are formally documented, along with mitigation strategies, for management review.
CC3.4.2	The security team monitors the security impact of emerging technologies and the impact of applicable laws or regulations through membership with professional associations, security forums, and technology institutes.
Monitoring Activities	
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	A management review meeting including executive leadership occurs on an annual basis to discuss long-term business goals, results of internal and external audits, and company risks.
CC4.1.2	ISMS control assessments are performed by a third-party at least annually to assess the maturity of the control environment, relevant risks, and opportunities for improvements. Results of the control assessments are reviewed by management and action plans are documented to address relevant findings and tracked to resolution.
CC4.1.3	Control self-assessments are performed by the IT risk and audit team at least annually to assess and evaluate that control activities related to criteria are in-place and operating effectively. Corrective actions are documented to address relevant findings and tracked to resolution.
CC4.1.4	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
CC4.2.1	A management review meeting including executive leadership occurs on an annual basis to discuss long-term business goals, results of internal and external audits, and company risks.
CC4.2.2	ISMS control assessments are performed by a third-party at least annually to assess the maturity of the control environment, relevant risks, and opportunities for improvements. Results of the control assessments are reviewed by management and action plans are documented to address relevant findings and tracked to resolution.
CC4.2.3	Control self-assessments are performed by the IT risk and audit team at least annually to assess and evaluate that control activities related to criteria are in-place and operating effectively. Corrective actions are documented to address relevant findings and tracked to resolution.
CC4.2.4	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
Control Activities	
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	A formal risk assessment is performed on an annual basis that includes an analysis of risk mitigation plans. The analysis considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
CC5.1.2	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above a tolerable threshold.

LabVantage

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	Assigned risk owners select and develop control activities over technology to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above a tolerable threshold.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	A documented employee handbook and policy manual are in place to communicate organizational policy statements and codes of conduct.
CC5.3.2	Employees are required to sign an acknowledgment form upon hire indicating they have been given access to the policy manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
CC5.3.3	An information security policy is formally documented that identifies the information required to support the functioning of internal control and achievement of objectives.
CC5.3.4	An employee sanction procedure is in place and documented within the employee manual to communicate disciplinary procedures for noncompliance with associated policies and procedures.
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.	
CC6.1.1	A documented access control policy is in place to provide guidance on account creation, modification, termination, and privileged access.
CC6.1.2	Documented standard build procedures are utilized for the installation of production systems.
CC6.1.3	Users are authenticated via a user account and password, two factor authentication, or multi-factor token before being granted access to system.
CC6.1.4	Administrative access privileges are restricted to user accounts accessible by authorized personnel for systems.
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.2.1	User access requests to the in-scope systems and applications are documented in the ticketing system and require approval from IT personnel.
CC6.2.2	Access to the in-scope systems is revoked for employees and clients as a component of the termination process and documented in the ticketing system.
CC6.2.3	A termination request form is in place to guide the termination process and includes procedures to help ensure that personnel access is revoked upon termination.
CC6.2.4	User access reviews of in-scope production systems are performed on an annual basis to help ensure that access to the application and production systems are restricted to authorized personnel.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	User access requests to the in-scope systems and applications are documented in the ticketing system and require approval from IT personnel.
CC6.3.2	Access to the in-scope systems is revoked for employees and clients as a component of the termination process and documented in the ticketing system.
CC6.3.3	A termination request form is in place to guide the termination process and includes procedures to help ensure that personnel access is revoked upon termination.

LabVantage

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
CC6.3.4	User access reviews of in-scope production systems are performed on an annual basis to help ensure that access to the application and production systems are restricted to authorized personnel.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
	AWS is responsible for implementing asset management procedures to discontinue logical and physical protections over physical IT assets and infrastructure at the end of their lifecycle.
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.	
	AWS is responsible for implementing asset management procedures to discontinue logical and physical protections over physical IT assets and infrastructure at the end of their lifecycle.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	Security groups are configured with access control rules to restrict inbound and outbound traffic within the AWS VPC.
CC6.6.2	A WAF is configured to filter traffic for customers into the production environment.
CC6.6.3	An encrypted VPN is required for remote access to in-scope systems.
CC6.6.4	The web servers utilize SSL encryption for web communication sessions.
CC6.6.5	Production data is encrypted at rest.
CC6.6.6	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
CC6.6.7	Employee workstations are encrypted.
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.	
CC6.7.1	A data encryption policy is formally documented and includes guidance to personnel for the encryption of data at rest and in transit.
CC6.7.2	A bring your own device (BYOD) policy is formally documented and includes guidance to personnel for the treatment of employee devices.
CC6.7.3	An FTP server is configured for the transfer of data.
CC6.7.4	An encrypted VPN is required for remote access to in-scope systems.
CC6.7.5	The web servers utilize SSL encryption for web communication sessions.
CC6.7.6	Production data is encrypted at rest.
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.	
CC6.8.1	Anti-malware software is configured for environments commonly susceptible to malicious attack and is configured to be updated daily, logged, and installed on employee workstations.
CC6.8.2	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
System Operations	

LabVantage

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
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.	
CC7.1.1	Documented standard build procedures are utilized for the installation of production systems.
CC7.1.2	A SEIM tool is utilized to monitor system events for in-scope systems to identify anomalies within network and system activity and configured to notify the 24X7 third-party Security Operations Center and other security personnel when suspicious network and system activity is identified by the tool.
CC7.1.3	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.2.1	Documented procedures for reporting security incidents are provided to employees to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.2.2	A third-party specialist performs a penetration test to identify threats and assess their potential impact to system security on an annual basis.
CC7.2.3	A SEIM tool is utilized to monitor system events for in-scope systems to identify anomalies within network and system activity and configured to notify the 24X7 third-party Security Operations Center and other security personnel when suspicious network and system activity is identified by the tool.
CC7.2.4	An enterprise monitoring application is utilized to monitor the availability and performance of production servers and network devices.
CC7.2.5	The enterprise monitoring application is configured to send notifications to IT and operations personnel when pre-defined thresholds are exceeded on monitored network devices.
CC7.2.6	Anti-malware software is configured for environments commonly susceptible to malicious attack and is configured to be updated daily, logged, and installed on employee workstations.
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.	
CC7.3.1	Documented procedures for reporting security incidents are provided to employees to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.3.2	Quality Team personnel track system incidents within an incident ticket to document system incidents, responses, and resolution.
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.	
CC7.4.1	Documented procedures for reporting security incidents are provided to employees to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.4.2	Quality Team personnel track system incidents within an incident ticket to document system incidents, responses, and resolution.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	Documented procedures for reporting security incidents are provided to employees to guide personnel in identifying and reporting failures, incidents, concerns, and other complaints.
CC7.5.2	Quality Team personnel track system incidents within an incident ticket to document system incidents, responses, and resolution.
CC7.5.3	A postmortem evaluation is completed for material security incidents found in production level services that include impact analysis, resolutions, lessons learned, and action items.
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.	

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
CC8.1.1	Documented policies and procedures are in place to guide personnel through the change management lifecycle.
CC8.1.2	The development team conducts biweekly sprint planning meetings to review upcoming changes.
CC8.1.3	Application changes are authorized, tested, and approved prior to implementation.
CC8.1.5	A ticketing system is in place for application changes to document, maintain, manage, and monitor change requests through implementation.
CC8.1.6	Testing and QA are performed in distinct environments that are logically separate from the production environment.
CC8.1.7	Version control software is in place and configured to restrict access to source code and provide rollback capabilities.
CC8.1.8	Write access to the version control software is restricted to user accounts accessible by authorized personnel.
CC8.1.9	The ability to implement changes to the production environment is restricted to user accounts accessible by authorized personnel.
Risk Mitigation	
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	A documented risk management policy is in place to guide personnel in identifying business objective risks, risks arising from potential business disruptions, assessing changes to the system, and developing risk management strategies as part of the risk assessment process.
CC9.1.2	Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
CC9.1.3	Business continuity and disaster recovery plans are tested on at least an annual basis.
CC9.1.4	Cyber insurance is in place to offset the potential financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	A documented risk management program policy is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks associated with vendors and business partners.
CC9.2.2	A formal risk assessment is performed on an annual basis that considers the impact of achieving business objective risks. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC9.2.3	A formal risk assessment is performed on an annual basis that considers the risks associated with vendors and business partners. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
CC9.2.4	A vendor due diligence assessment is required to be completed for vendors that assesses the potential risks and vulnerabilities as a component of the onboarding process.
CC9.2.5	A standard service agreement that addresses confidentiality and data protection requirements is required to be in place prior to sharing information designated as confidential with third parties.
Availability	
• **A1.1** The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	
A1.1.1	Documented policies and procedures are in place to help guide operations personnel in the data backup, disaster recovery, and business continuity processes.
A1.1.2	A documented disaster recovery and business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

LabVantage

LabVantage Security Addendum

Control #	SOC 2 Control Requirements
A1.1.3	An enterprise monitoring application is utilized to monitor the availability and performance of production servers and network devices.
A1.1.4	The enterprise monitoring application is configured to send notifications to IT and operations personnel when pre-defined thresholds are exceeded on monitored network devices.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	
A1.2.1	A documented risk management program policy is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks associated with environmental threats.
A1.2.2	A formal risk assessment is performed on an annual basis that considers the risks associated with environmental threats. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.
A1.2.3	Documented policies and procedures are in place to help guide operations personnel in the data backup and recovery process.
A1.2.4	Automated backup systems are utilized to perform scheduled system backups of production data and systems.
A1.2.5	The automated backup systems are configured to send e-mail alert notifications to IT and operations personnel regarding backup job summary and completion status. The backup job summary is reviewed daily and failed jobs are subsequently re-run until successful.
A1.2.6	An enterprise monitoring application is utilized to monitor the availability and performance of production servers and network devices.
A1.2.7	The enterprise monitoring application is configured to send notifications to IT and operations personnel when pre-defined thresholds are exceeded on monitored network devices.
A1.2.8	Redundancy is built into the architecture to provide failover of operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	
A1.3.1	Business continuity and disaster recovery plans are tested on at least an annual basis.
Confidentiality	
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	
C1.1.1	An information security policy is formally documented that identifies the information required to support the functioning of internal control and achievement of objectives.
C1.1.2	Documented data classification, data protection, and data retention policies are formally documented to guide personnel in the handling of confidential data.
C1.1.3	Administrative access privileges within the AWS cloud platform management console are restricted to user accounts accessible by authorized personnel.
C1.1.4	Administrative access privileges within the AWS RDS production databases are restricted to user accounts accessible by authorized personnel.
C1.1.5	An encrypted VPN is required for remote access to in-scope systems.
C1.1.6	The web servers utilize SSL encryption for web communication sessions.
C1.1.7	Production data is encrypted at rest.
C1.1.8	Redundancy is built into the architecture to provide failover of operations to alternate infrastructure in the event normal processing infrastructure becomes unavailable.

Control #	SOC 2 Control Requirements
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	
C1.2.1	Documented data destruction policies and procedures are in place that include the following: • Identifying information requiring destruction when the end of the retention period is reached • Erasing or destroying information that has been identified for destruction
C1.2.2	Customer data is deleted upon customer request subject to applicable law.
C1.2.4	Backups of databases are configured to be deleted per a defined schedule.

18) ISO 27001 Technical and Organizational Security Controls

a) Measures of pseudonymization and encryption of personal data

- Encryption is implemented on all company PCs and servers.
- Personal business contact information, stored in VantageCare, is able to be pseudonymized as a standard function of the software.

b) Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- The VantageCare system, where personal business contact data is stored:
  - Is configured for high-availability and automatic failover
  - Is available 24/7/365
  - Configured with 4-hour backup and restore capabilities
  - Requires unique username and password for access
  - Uses secure data transmission
  - Audit trails and event logs turned on to capture changes and events
  - Support staff is available 24/7/365

c) Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- The VantageCare system is configured for a 4-hour image backup that is retained for a minimum of 14 days. VantageCare is the customer portal where the business personal data is located.
- Computer systems are configured for a daily image backup that is retained for a minimum of 14 days.

d) Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

- The Quality department executes annual internal audits to verify compliance to IT security procedures.
- LabVantage undergoes an annual audit by a third-party auditing company to verify ongong compliance to security governance, management, and ISO 27001.
- Annual infrastructure penetration testing is conducted and issues addressed.

e) Measures for user identification and authorization

- Unique username and passwords (the user must set their own passwords) are used to clearly identify the user.
- Shared user accounts and sharing of passwords are not allowed and are against company policy.
- Multi-factor authentication is implemented.
- Password policy is in place to require passwords to meet the following three out of four requirements: 1) upper case letter, 2) lower case letter, 3) number, 4) special character), minimum password length. The password policy also requires periodic password changes and password history to prevent the reuse of old passwords.
- Users are assigned roles and permissions that are applicable to their job function and which restrict access to areas of data that are not needed.

- User access to PCs, systems, and servers are terminated on the last day of employement.
- Event logs and audit trails are implemented to log user access (successful and unsuccessful) to a system and activities once within the system.
- Periodic user reviews are executed to ensure:
  - Only authorized users have access to systems.
  - Terminated user accounts are disabled or purged.

f) Measures for the protection of data during transmission

- Emails are scanned, quarantined if needed, and monitored using anti-virus, anti-spam, and phishing software.
- Secure data transmission is implemented using HTTPS, SSL certificates and VPN (Virtual Private Network).

g) Measures for the protection of data during storage

- Encryption is implemented on all company PCs and servers.
- Virus and anti-malware softare is implemented on company PCs and servers with automatic definition updates.
- Automatic screen lock is implemented on PCs to lock the PC when idle and screen unlock requires a password.

h) Measures for ensuring physical security of locations at which personal data are processed

- The data center has access controls using a card access system to allow only authorized access.
- All access points are monitored via a closed-circuit TV and centrally monitored.

i) Measures for ensuring events logging

- Event logging is turned on for all successful and unsuccessful login attempts.
- Event log audit trail is read-only to prevent alterations.

j) Measures for ensuring system configuration, including default configuration

- Change control process is in place for any changes to the system.
- Audit trails are turned on to capture and document system configuration changes.
- Users are provided with the least privilege permissions needed to perform their job functions, hence only authorized users with the appropriate permissions can make changes.
- Systems are implemented / configured with the appropriate security permissions and user roles.

k) Measures for internal IT and IT security governance and management

- The Quality department executes annual internal audits to verify compliance to IT security procedures.
- LabVantage undergoes an annual audit by a third-party auditing company to verify onging compliance to security governance, management, and ISO 27001.

l) Measures for certification/assurance of processes and products

- For software releases, Quality oversees the complete Software Development Life Cycle and validation process and will not release software unless all items are in place and all activities have been completed. This includes periodic auditing and verifications.
- For the Quality Management System and the Information Security Management System, Quality oversees and continuously verifies compliance to the various security and non-security processes and procedures to ensure compliance to those processes and procedures.

m) Measures for ensuring data minimization

- Data is only used for the purpose it is collected.
- Access to the data is restricted to only those who need it and it is controlled by roles and permissions.
- Data is deleted 1) at the request of the data subject, 2) when the data is no longer needed, or 3) when the data retention period is reached.

n) Measures for ensuring data quality

- 21 CFR Part 11 / Annex 11 compliant audit trails are turned on for all data changes that capture

the username, date, time, previous value, changed value, and change reason.
- User roles and permissions are configured and assigned to the users to manage (allow or prevent) access to the data. This includes viewing, editing, and deletion of the data.

o) Measures for ensuring limited data retention
- A data retention policy is in place that governs the retention period of data, including personal data.
- Personal data will be kept for the minimum required time and deleted when it is no longer needed.
- Data subjects may request their data to be deleted (request to be forgotten).

p) Measures for ensuring accountability
- Unique username and passwords are used to clearly identify each user.
- Shared user accounts and sharing of passwords are not allowed and against company policy.
- Users are assigned roles and permissions that are applicable to their job functions to restrict access to areas of data that is not needed.
- 21 CFR Part 11 / Annex 11 compliant audit trails are turned on for all data changes that capture the username, date, time, previous value, changed value, and change reason.

q) Measures for allowing data portability and ensuring erasure
- The system allows that personal business contact information is able to be edited, exported in a human readable format, pseudonymized, or purged.

r) Measures for reporting a data breach or security issue
- There is a procedure in place to report (including reporting to the Data Breach Team, the data subject, or the Supervisory Authority), log, contain, investigate and remediate security breaches, data loss, or other similar issues / events.

s) Measures to control company assets
- PCs are tagged, provided for use, and then returned when no longer needed by the user.
- Destruction of hardware storing data is managed by: 1) the data is first purged, then 2) the hardware is physically destroyed beyond use.
- Encryption is implemented on company PCs and servers.
- Virus and anti-malware software is implemented on company PCs and servers with automatic definition updates.
- Automatic screen lock is implemented on PCs to lock the PC when idle and screen unlock requires a password.
- PCs and servers are automatically backed up to prevent data loss.
- USB ports are set to read-only to prevent unauthorized export of data or software.
- Asset owners shall not allow unauthorized people to use company assets.

t) Measures to control network and office security
- Systems and networks are located behind firewalls that are configured to prevent unauthorized access.
- Network monitoring software is running to monitor the network for issues, including unauthorized access, security breaches, or viruses.
- The office areas are secure via locked doors, accessible using a card access system, and monitored by closed-circuit TV.
- The office is monitored after-hours by a central monitoring station for unauthorized access and fire.
- Sensitive and confidential areas are secured to restrict access to only authorized people.
- Visitors are monitored while in the office area.
- Network penetration testing is executed to identify possible vulnerabilities and remediated as needed.

u) Measures to control personal, confidential and company data
- Data is classified in the following categories and controlled / restricted as needed: Public, Internal Use, Restricted, Confidential, and Confidential – Personal.

- Pseudonymisation and anonymization of personal data is implemented when needed.
- There is a procedure in place to opt out or correct personal data.

19) Amazon Web Services (AWS) Technical and Organizational Measures

The below technical and organisational measures are implemented by AWS and apply to LabVantage SaaS.

General Note: AWS is compliant to several ISO requirements and other regulations that address data security-related and data security and undergo annual audits for compliance verification. This includes, but is not limited to:

- ISO 9001:2015 Certification
- ISO 27001:2013 Certification
- ISO 27017:2015 Certification
- ISO 27018:2019 Certification
- System and Organization Controls (SOC) 2 Report

AWS controls include, but are not limited to:

Data Transmission

- Secure data transmission is implemented using HTTPS, SSL certificates, and VPN (Virtual Private Network).

Network and Data Center Security

- Systems and networks are located behind firewalls that are configured to prevent unauthorized access.
- Network monitoring software is running to monitor the network for issues, including unauthorized access, security breaches, or viruses.
- Data Center areas are secure via locked doors and security monitoring systems.
- Sensitive and confidential areas are secured to restrict access to only authorized people.
- Visitors are monitored while in the office area.
- Network penetration testing is executed to identify possible vulnerabilities and remediated as needed.

Last updated: 22 Oct 2025