LANEXO® System Security Brief

Product Overview

The LANEXO® Lab Inventory, Safety & Compliance Management System is designed to create efficiencies, improve safety and facilitate compliance in highly regulated analytical and research laboratories. It is delivered as Software as a Service (SaaS) solution that helps customers efficiently manage laboratory consumables inventory while maintaining high standards in executing processes and staying compliant with GxP and safety requirements. The LANEXO® System includes a Mobile Application, a Web Application, RFID labels and user access cards. The system is developed in accordance with the Merck KGaA, Darmstadt, Germany Group information protection management system, which is based on ISO 27001 and comprises security guidelines as well as organizational and technical measures to prevent and address IT security incidents. This document is intended to provide a comprehensive summary of the current information security posture of the LANEXO® System. We are committed to doing our best to meet changing requirements and standards; therefore, this is a living document that may be revised to reflect such changes.

Information Security Governance

Information Classification

All information assets associated with the LANEXO® System are classified based on our 5-step information classification scheme. The current classification of the LANEXO® System's information is set as "Confidential" based on initial business requirements analysis. Information assets will be reclassified on a regular basis. It is recommended that they be further assessed and classified when LANEXO® System is implemented at a customer site.

Risk Management and Compliance

The LANEXO® System facilitates 21 CFR Part 11 compliance by meeting applicable end user requirements based on intended use and developmental approach following the GAMP 5 model to fulfill regulatory requirements. The system validation process in development ensures that all system components and associated processes are assessed for risks, which are then mitigated and documented. Similar to regulatory risks, security risks are assessed following a risk treatment plan. A continual process to review, examine and test security controls has been put in place to maintain a desirable security status. Privacy and protection of personally identifiable information are ensured as required in relevant legislation and regulation where applicable.

Application Security

The LANEXO® System's Web and Mobile applications are built on an industry-standard secure application architecture framework. Security by Design principles of OWASP are followed to ensure that the system's applications are secure and built with adequate controls to reduce the risk of any foreseeable threat.

Secure Application Architecture

The Web application's backend is built using an event-sourcing architecture that allows storage of all states of the system caused by events and to permit effective restoration of the system to the state it was in before an adverse event occurred. A few key security controls and features of the Web application are listed below.

- **Identification of users:** The application uses unique IDs to identify users and trace their actions according to their digital signatures. Physical identities of users are verified by the LANEXO® access cards. As the default, group IDs and shared IDs are disabled.
- **Authentication & authorization:** Two-factor authentication is implemented by restricting access to users who possess a physical access card containing a private key and a valid email/password combination. Role-based access control is implemented in the Web application to ensure that resources can be accessed only on a "need-to-know" and "least-privileged" basis.
- **Encryption of data at rest:** Storage of data in the database uses industry-leading encryption technologies such as Transparent Data Encryption (TDE). File system storage adopts vendor-specified (Amazon Web Services) encryption techniques such as S3 CSE*CSMK. All passwords are stored in salted and hashed form.
- **Encryption of data in transit:** TLS1.1+ requirements (DHE or RSA – Key Exchange Algorithm; SHA-256 – Hash function) are met to encrypt data in transit. The AES-256 Data Encryption Algorithm is used based on SSL policy recommendations by the vendor (AWS). SSL/TLS certificates are stored separately.

Secure Application Development

LANEXO® System application development follows a secure software development lifecycle to ensure both the fulfillment of security requirements for the application and the security of the systems and information involved in development. The development of the system rigorously follows a stage gate product development process that inherently screens for fulfillment of security, regulatory and compliance requirements. Our IT department's guidelines for secure application development are followed. A few key highlights of the secure application development process are listed below.

- **Requirements and security risk:** Alongside the business and functional requirements of the LANEXO® System, the security requirements were determined and applied in the design specifications. An initial risk assessment identified the key security risks associated with the application, outlining the security controls required to address the information security triad of Confidentiality, Integrity and Availability.
- **Security by Design:** The design and development of the LANEXO® System's Web and Mobile applications followed specifications referencing the OWASP Top 10 and OWASP Mobile Top 10 security risks. General programming best practices were adopted in the development of the application.
- **Application Testing:** Specific security functions (based on OWASP Top 10 threats) implemented in the application are tested. A cyclic penetration testing exercise is performed on the application ecosystem to add an additional protection check, which complements the secure coding paradigm. Code reviews are performed to ensure that best coding practices are followed.

Infrastructure and System Security

The LANEXO® System is hosted on the Amazon Web Services (AWS) Cloud and is governed by our SLA with AWS. AWS is regularly audited by different independent third-party organizations to maintain their ISO certifications (9000, 27001 27018) and SOC reports. In addition, we performed a supplier audit for relevant evidence, certificates and controls. A few key measures taken to secure the LANEXO® System are listed below.

Secure AWS Design

The LANEXO® System follows a best-practice approach as defined in "The AWS Well Architecture Framework" and has additional security controls around the AWS services and APIs used for developing the LANEXO® System. Some of the key aspects that are considered in the design are listed below.

- Encrypting all endpoints/APIs and using a secure process to manage keys/secrets
- Restricting internet access only to required AWS services and using private subnetting for critical AWS services and resources
- Continuous monitoring of AWS services for exceptions and events
- Configuring the system to detect failure and to self-heal
- Access to AWS accounts and resources for administrative/operational tasks are tightly controlled by our Enterprise IT standards and policies.

System Security

In addition to leveraging the built-in security controls and trusts available within the AWS Cloud, additional solutions are used to enhance the security of the system. The list below discusses a few such solutions.

- **Secure configuration:** The LANEXO® System employs established standard secure images of operating systems and software tools to minimize threat/vulnerability exposure. Operating system images are hardened and regularly updated for any recent vulnerabilities and attack vectors. Infrastructure-related and application configurations are maintained in separate repositories and version controlled.
- **Firewall & malware protection:** At the application level, an industry-standard web-application firewall (WAF) has been configured to protect the system from the OWASP Top 10 threats. An additional commercial malware protection solution is considered to provide host- and application-based malware protection. For perimeter defense against malware, AWS trust controls are leveraged. A process for regularly updating the malware signatures has been put in place.
- **Logging & monitoring:** The LANEXO® System is securely maintained using standard monitoring solutions and tools to support early identification of potential losses of information. Logging of events and incidents is activated at both the application and infrastructure system levels. Log files are regularly monitored and analyzed for suspicious events, anomalies and deviations. Thresholds and metrics defining anomalies and deviations are set in the tools to provide alerts.

It is recommended that the above information be further assessed to determine if the LANEXO® System might need additional controls based on intended use by customers.