Security Overview

SAAS Provider & Data Center Policies and Procedures for Atrixware, LLC

Introduction

This document provides a comprehensive overview of the security policies and procedures enacted by both Atrixware and its partner data center to ensure the confidentiality, integrity, and availability of client data and services. It outlines the principles and practices that guide the development, deployment, and maintenance of secure software and infrastructure.

Scope

The policies and procedures outlined in this document apply to Atrixware and its employees, contractors, and third-party vendors who have access to client data or systems. It covers all aspects of security, including physical security, network security, application security, and data protection.

Application Access Management Policies & Procedures

Logging into the Axis LMS as an administrator, manager, or user necessitates entering a unique username and password. The administrator and manager portals can be set to automatically log out administrators and managers after a period of inactivity. All actions and changes made by administrators and managers are logged and can be accessed by the client through various logs and changelogs within the system.

User access can optionally be configured to utilize two-factor authentication via email/SMS message for added security. Each user must log in using a unique user account, and administrators can set optional limits on the number of devices a user can log in from, the number of concurrent active sessions, and set automatic logout for inactive users. Optional password expiration settings prevent users from having stale passwords, and failed login attempt settings help to prevent brute-force attacks on user accounts. All login attempts, user actions, IP addresses, and device information are recorded and logged within the LMS system for auditing purposes.

The client's Axis LMS can optionally be configured to limit access to the LMS to specific IP addresses (whitelist), or to completely block (blacklist) specific IP addresses.

Application Data Policies & Procedures

All data transferred to and from Axis LMS is encrypted using Transport Layer Security (TLS) 1.3 encryption, providing robust security measures that ensure the confidentiality and integrity of information exchanged between administrators, users, and the LMS.

The *Gold Secure LMS Hosting* and the *HIPAA compliant Platinum Secure LMS hosting* packages include hardware RAID with encryption, ensuring that all application data is encrypted "at-rest" for enhanced security.

Provider Access Management Policies & Procedures

Atrixware follows the principles of “least privilege” when it comes to access to client’s Axis LMS, hosting server, software code-base, and underlying data.

- Sales and Customer Service representatives have access to the client’s administrative contact information and may access the client’s Axis LMS with the express permission of the client.
- Level 1 Support Technicians have access to the client’s administrative contact information and full access to the client’s Axis LMS.
- Level 2-3 Support Technicians, Server Administrators, and Software Developers have access to the client’s hosting server, software code-base, and underlying data.

Provider Data Retention Policies & Procedures

All client data, with the exception of client administrative contact data, is promptly removed from hosting servers upon termination of service. Additionally, all client data is purged from server backups within 30 days of termination of service.

Provider Secure Software Development Policies & Procedures

Atrixware embraces an Agile development methodology, prioritizing the implementation of best practices to ensure the creation of secure code. These practices include robust input validation, meticulous data sanitization, thorough output encoding, and comprehensive error handling.

The development process begins on an isolated development server. Each update, feature, or revision undergoes static analysis as well as internal quality assurance testing. Once the code meets standards and all new features/changes have been thoroughly tested, it is deployed to a sandbox "semi-production" server. Here, clients have the opportunity to preview and thoroughly test new features, ensuring a seamless transition to their production systems.

The frequency of releases varies depending on the patch's nature and purpose. Vulnerabilities and security issues can be identified, corrected, and patched within hours if not minutes. Bugs that don't impact the overall system stability or data reliability are typically addressed within 1-2 business days. Non-critical bugs or feature releases may be included in larger patches with longer release intervals.

Data Center Governing Policies & Procedures

All data center governing policies and procedures have been developed to adhere to the NIST 800-53 standard, a cybersecurity framework which is widely recognized as best practice within the industry and designed to ensure organizations comply with the U.S. Federal Information Security Modernization Act.

The NIST 800-53 framework consist of five phases:

- Identify - find and evaluate all cybersecurity risks
- Protect - design and implement safeguards to ensure delivery of critical services
- Detect - identify, detect, and analyze a cybersecurity event
- Respond - respond and recover to a cybersecurity event as needed
- Recover - identify, restore, and improve resilience for any services impaired

In order to ensure compliance within the NIST 800-53 standard, as well as ensure the highest standards of service, our data center has implemented the following policies and procedures:

- Implement formal risk management policies and procedures including accessing operations, reporting, and compliance risks, and update these policies on an annual basis.
- Conduct a formal risk assessment on annual basis, reviewing:
  - Company operational, financial, reporting, and compliance objectives and risks.
  - Identifying changes to the company, technology, or environment that may allow for new or additional risk.
  - Conduct a complete assessment of third-party risk.
  - Assign a risk rating and action plan for all identified risks.

- Conduct monthly Incident Outcomes and Action Review (IOAR) meetings in order to evaluate deficiencies, develop new control activities, track identified risks, and communicate any relevant changes to controls and/or employees responsible.
- Annually review business continuity and disaster recovery plans that outline steps to be taken in order to continue service and respond to disasters.
- Conduct annual tabletop exercises of system redundancy using the business continuity and disaster recovery plans as a framework for resolving tests to ensure comprehensive coverage.

For a full list of data center certifications and compliance reports, please refer to https://www.liquidweb.com/about-us/policies/certifications/

Data Center Infrastructure Policies & Procedures

Data centers are engineered to have redundancy at each level, ensuring that a failure at any point will not impact client servers. Power is conditioned and dependable, thanks to centralized Uninterruptible Power Supplies (UPS) systems supported by generators. Data centers exclusively rely on premium Tier-1 bandwidth providers, guaranteeing minimal latency and rapid connections to all parts of the global internet.

Environmental processing systems include upflow and downflow CRAC units that include pumped refrigerant systems to help ensure maximum efficiency while maintaining precision server inlet temperature. Temperature and humidity are precisely regulated year round to ensure optimal equipment reliability. Each unit contains independent compressors and cooling loops to further enhance fault tolerance and reliability. Air filtration systems actively remove foreign particles from circulation and cycle the entire data center air supply in a matter of minutes.

Hosting services are primarily delivered through virtual machines, which are shared among multiple clients. Dedicated servers are also available, offering private resources allocated entirely to a single client, as part of the *HIPAA compliant Platinum Secure hosting* package.

Data Center Data Access/Storage Policies & Procedures

The data center does not manage, access, transfer, or move client data or content in any way. Typically, all client data is stored in a US data center located in Lansing, MI. However, clients have the option to host Axis LMS outside the US. In such cases, all client data is stored in an EU data center located in Amsterdam, NL.

Data Center Backup Policies & Procedures

All servers are fully backed each night and stored on-site within the data center's cloud storage service. Full server backups are retained for up to 30 days and include backups for the last 7 days, along with 4 weekly backups. All backup data is transferred from the hosting server to the backup cloud storage via a secure private network. Off-site backup storage and additional backup retention options are available as part of the *Gold Secure LMS Hosting* and the *HIPAA compliant Platinum Secure LMS hosting* packages.

Data Center Network Security Policies & Procedures

The data center network is engineered to meet the needs of clients who require top-notch network performance. The design prioritizes redundancy, enabling the network to swiftly recover from failures without disrupting connectivity. The redundancy structure is multi-tiered, featuring N+1 internal device elements and fully redundant chassis, ensuring that any routing device can fail without affecting client data connectivity. All core routing and switching equipment utilize cutting-edge Cisco products.

During commissioning, all servers undergo a hardening process that adheres to industry best practices, ensuring robust security configurations. Each server is also safeguarded by both a software and cloud firewall, which ensures that all server traffic is meticulously filtered and regulated. They are also shielded by a software-based intrusion detection system that constantly monitors server and user processes, identifies excessive connections, defends against common attacks like SYN floods, port scans, and brute-force attempts, and regularly conducts essential security and setting assessments throughout the server. Furthermore, all servers are subject to ongoing scans for malware

Additional security measures such as hardware firewalls, fully managed intrusion detection systems, advanced DDoS attack protections, monthly external vulnerability scans, and advanced server hardening are available as part of the *Gold Secure LMS Hosting* and the *HIPAA compliant Platinum Secure LMS hosting* packages.

Data Center Physical Security Policies & Procedures

Our data center partners adhere to a strict series of policies to ensure that physical access to the data center, along with any systems within, are restricted to relevant authorized personnel only.

Specialized electronic security systems control access to the data center and are accompanied by a full complement of motion detecting security cameras which monitors the entire facility at all times. Surveillance cameras are placed throughout the data center to record all activity throughout the facility, work areas, and server rooms. Surveillance video is retained for a minimum of 90 days. Badge access systems used throughout the facility log all successful and unsuccessful access attempts and retain those logs for a minimum of 90 days.

The data centers' external walls are reinforced poured concrete and have highly trained technicians on-site 24 hours a day to provide fast incident response times. All visitors are required to present a valid photo ID, are provided a visitor ID badge, and are escorted for the duration of their visit. Access to telecom, central switching equipment, and individual workstations are restricted to authorized personnel.

To ensure that only current, authorized personnel have access to relevant systems and areas, the on-site security team conducts monthly audits. These audits cover unused badges, failed badge access attempts, added and deleted badges, and any changes made to badge access permissions.

All data center employees are subject to background checks upon hire and undergo training on general workstation guidelines (such as clean desk policies and situational awareness policies), security awareness (including tailgating and best practices), and are expected to adhere to a formal acceptable use policy. User access reviews are performed annually by all department heads to determine if access privileges are appropriate and any changes are related to the security team during this process. All user access request changes, including temporary access changes, must be submitted, approved, and performed by the data center security team.

The data center utilizes a formal inventory system to monitor all hardware used within the facility and its environment. Regular audits are conducted to ensure accuracy and compliance. Hardware decommission policies are in place to ensure that all decommissioned hardware is tracked and stored in a physically secured location until it undergoes sanitization and destruction. A hardware sanitization policy is in place that outlines the procedures for the irreversible removal of all data prior to disposal of hardware.

Contractor and Third-Party Vendor Security Policies & Procedures

Atrixware does not engage in partnerships or contracts with external contractors, providers, or third-party vendors, beyond the aforementioned data center partner, who have access to client applications, data, or servers, unless access is explicitly authorized by the client.