LICENSALE.COM
global medtech registration system

Introduction

Licensale 2.0 is a cloud based data management system hosted on Amazon AWS cloud. The following document outlines the security strategies Licensale 2.0 implements in addition to the following AWS security protocols highlighted below

SECURE DESIGN

SITE SELECTION

Prior to choosing a location, AWS performs initial environmental and geographic assessments. Data center locations are carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. Our Availability Zones are built to be independent and physically separated from one another.

REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, AWS customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

CAPACITY PLANNING

AWS continuously monitors service usage to deploy infrastructure to support our availability commitments and requirements. AWS maintains a capacity planning model that assesses our infrastructure usage and demands at least monthly. This model supports planning of future demands and includes considerations such as information processing, telecommunications, and audit log storage.

BUSINESS CONTINUITY & DISASTER RECOVERY

BUSINESS CONTINUITY PLAN

The AWS Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, AWS documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

PANDEMIC RESPONSE

AWS incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

PHYSICAL ACCESS

EMPLOYEE DATA CENTER ACCESS

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

THIRD-PARTY DATA CENTER ACCESS

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

AWS GOVCLOUD DATA CENTER ACCESS

Physical access to data centers in AWS GovCloud (US) is restricted to employees who have been validated as being US citizens.

MONITORING & LOGGING

DATA CENTER ACCESS REVIEW

Access to data centers is regularly reviewed. Access is automatically revoked when an employee’s record is terminated in Amazon’s HR system. In addition, when an employee or

contractor's access expires in accordance with the approved request duration, his or her access is revoked, even if he or she continues to be an employee of Amazon.

DATA CENTER ACCESS LOGS

Physical access to AWS data centers is logged, monitored, and retained. AWS correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

DATA CENTER ACCESS MONITORING

We monitor our data centers using our global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV

Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

DATA CENTER ENTRY POINTS

Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

INTRUSION DETECTION

Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to

server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 AWS Security Operations Centers for immediate logging, analysis, and response.

DEVICE MANAGEMENT

ASSET MANAGEMENT

AWS assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for AWS-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

MEDIA DESTRUCTION

Media storage devices used to store customer data are classified by AWS as Critical and treated accordingly, as high impact, throughout their life-cycles. AWS has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, AWS decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from AWS control until it has been securely decommissioned.

OPERATIONAL SUPPORT SYSTEMS

POWER

Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with

back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

CLIMATE AND TEMPERATURE

AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION

AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION

In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

EQUIPMENT MAINTENANCE

AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

ENVIRONMENT MANAGEMENT

AWS monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information

provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

ONGOING DATA CENTER RISK MANAGEMENT

The AWS Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

THIRD-PARTY SECURITY ATTESTATION

Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

LICENSALE'S INTERNAL SECURITY MEASURES

APPLICATION ARCHITECTURE

Licensale 2.0 is a multi-layered MVC application with data accessible only from the data layer and no data is directly accessed from the view layer. The back-end server is three layer MVC with Spring java framework. The front-end server was developed with ReactJS framework.

ENCRYPTION OVER THE WIRE

Communications to and from all sensitive areas of the application are secured by 256-bit SSL certificates. The database is also encrypted. User passwords are stored using a one-way hashing algorithm (SHA-256), transmitted via SSL/using only TLSv1.2 and TLSv1.3, and never transmitted unencrypted.

SECURITY PROCEDURES, POLICIES AND LOGIN AUTHENTICATION

Authentication is managed using the OAuth2 protocol thus User credentials are not stored or managed locally, preventing the possibility of credentials being physically compromised. Passwords are not logged under any circumstances.

Passwords are forced to expire after 6 months of use (expiry duration can be adjusted to reflect industry standard as it evolves); to encourage strong passwords on LS2.0, all user passwords must contain letters, numbers, and non-alphanumeric characters and be at least 8 characters long. Passwords cannot be reused.

The LS2.0 system automatically logs users out after a period of a period of inactivity. In the event of consecutive failed login attempts, users are locked out (lockout period can be adjusted to reflect industry standard as it evolves).

Passwords reset links are delivered automatically via email to the requesting User when users go through account recovery. During the reset period, reset password is temporarily set to a random value (which must be changed on first use)

User access log entries are maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (viewed, edited, etc.) and source IP address. Log is kept for a minimum of 90 days in a secure area to prevent tampering.

ACCESS TO AWS

Access to AWS dashboard is restricted to “need” to know basis” following the “least privilege” security principles. Only 2 IAM users are able to log in to the AWS dashboard to service and update the production server.

CODE REVIEW

All code is reviewed on a regular basis by at least one other developer against the security requirements and secure coding guidelines.

BACKUPS

Automatic backups of the database are taken daily. This data is stored and encrypted within the production server database.

PERMISSIONS

The highlights of User Permission on LS2.0 is as follows

- Only “Super Admin” users within Arazy Group have access to the full spectrum of functionalities on the production servers only for the purposes of completing tasks unavailable to Lead Clients (e.g. creating all types of user profiles, creating applications, uploading/updating compliance information and requirements in different regulatory markets as they change). The super admin role is limited to 3 users within Arazy Group; all other users within Arazy Group have limited access to applications, documents and products as Lead Expert users (only have access to these locations if they are designated as Lead Expert).

- The “Lead Client” role is able to access all information that belongs to their company including viewing all applications, products, documents uploaded by users of their company and viewing profile information (name, phone number, email address) of all users within their company. The Lead client is able to request password changes and disable users which prevents inactivated user profiles from logging in.
- The “Client” role users are only able to access applications and documents that Lead clients have shared with them. The lead client is able to remove client users from any application at any time
- “Lead Expert” role users which review applications on behalf of clients are only able to access applications assigned to them and see all the documents that are included in the assigned application.
- “Expert” role users are only able to assist on and have access only to individual documents/compliance information if they have been shared the individual documents/compliance information for a given application.