CSX Security and Data Protection Overview

Last Updated: 20220920.1

CSX is committed to ensuring compliance to best practice as well as any security and data protection regulations. CSX has in place a wide variety of technical and organisational controls to ensure such compliance.

CSX organizational controls

CSX, as a subsidiary of HitIQ Ltd, operates under the HitIQ ISO27001 Information Security Management System (ISMS) and ISO13485 Quality Management System (QMS) for organizational and technical controls over IT security and data privacy. HitIQ has achieved certification from BSI for ISO13485 and is in the process of moving toward certification of the ISO27001 ISMS.

Privacy Regulation Compliance

CSX is compliant to the relevant privacy regulations in the countries of sale. Regulations such as GDPR, HIPAA, UK GDPR, Australian Privacy Act, as well as others are accounted for in the various procedures and technical controls on the products and the organization.

CSX System Topology

CSX Systems products are comprised of a set of mobile applications and web portals.

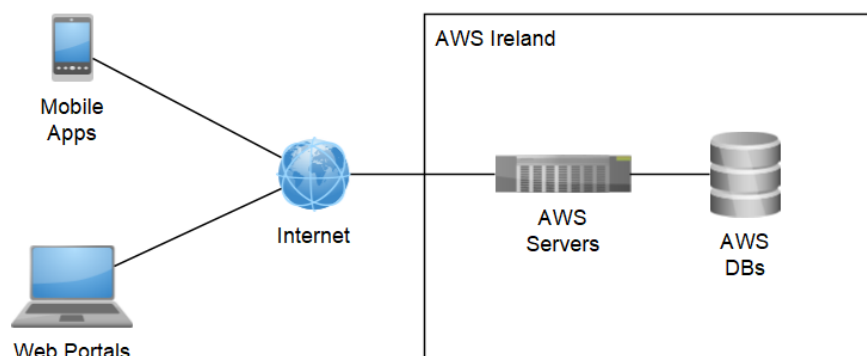CSX servers and databases are hosted in AWS Ireland.

Figure 1 -CSX System Topology

Specific Technical Controls for Customer Data

CSX Systems utilize current best practices for data encryption in transit and at rest.

TLS1.2 is used for data transmission between systems, including mobile apps and in web browsers. All network traffic uses HTTPS (port 443).

![HIT·IQ logo]

Data is encrypted at rest in AWS managed databases using AES-256-GCM symmetric encryption in private subnets.

The mobile applications, web applications, and APIs use Okta for user authentication.
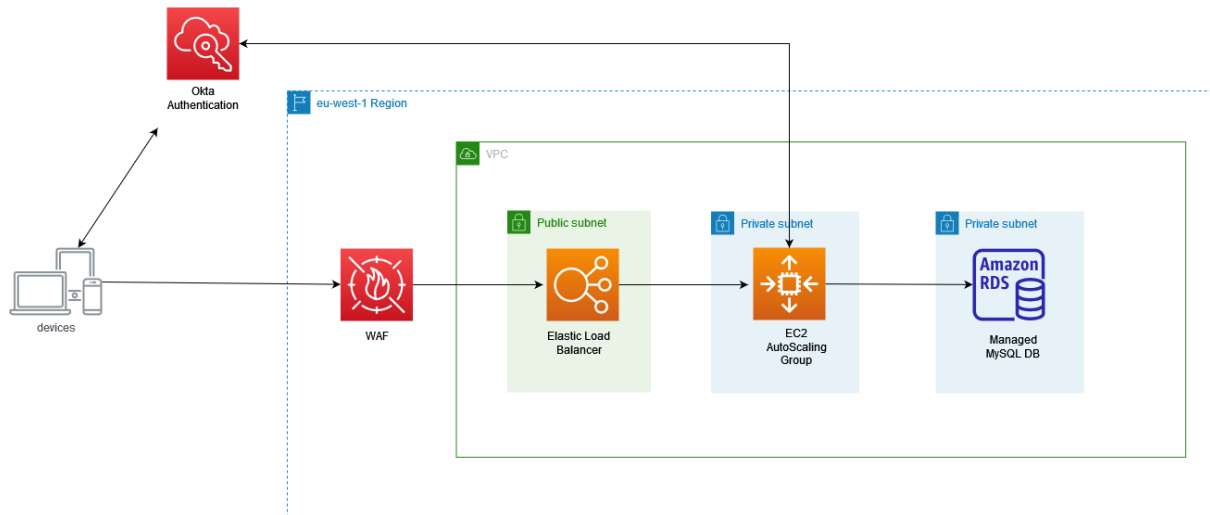

Figure 2 - CSX Backend Diagram

The mobile apps and web portal access data using an API and application hosted on EC2 instances.

A Web Application Firewall (WAF) and Elastic Load Balancing provide security and scalability features to the system.

Backup and Disaster Recovery

CSX databases are run on AWS RDS which provides high durability, availability, and reliability. CSX backs up RDS daily and can restore backups if necessary.

Access Controls

Access to CSX customer data is restricted within CSX/HitIQ. Access to customer data is governed by the provision of consent by the customer under contract and/or under specific support requests. HitIQ system administrators and support engineers can only access customer data upon request by customers for support. HitIQ administrators may also process data for backup/restore or database administration, but only in aggregate.