Version 1.9

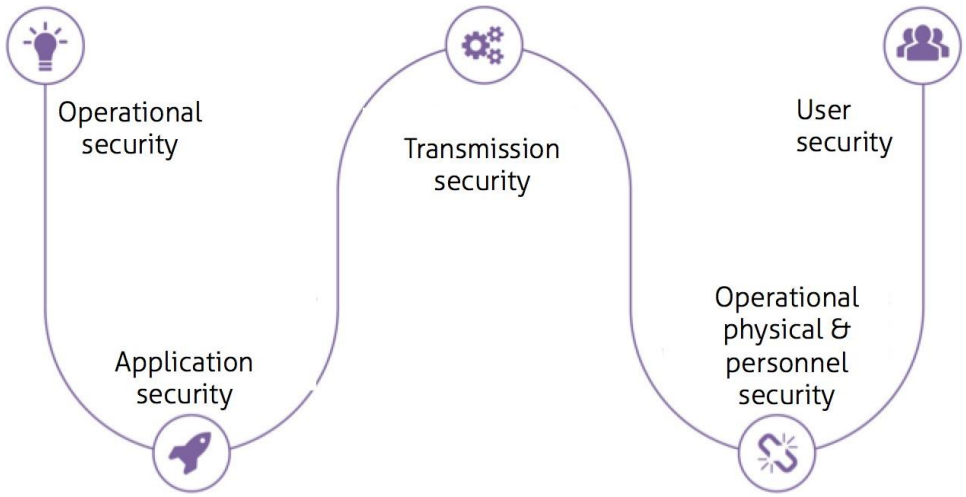
Cloud Platform Security Fact Sheet

This document is not for general circulation or public disclosure.
Please do not circulate or distribute this document.

CHSPOS understands that data is among the most strategic and important assets an organisation has. Therefore we put the highest priority on maintaining the security and privacy of our customers' data.

CHSPOS SaaS's enterprise-level security features manage operational security, user security, data security, application security and transmission security. Underlying it all is an environment of continuous monitoring and improvement. Together, these capabilities provide a complete security solution.

We use a multi-faceted approach to enforce security and we constantly monitor and search for new threats.



Contents

Operational Security

Physical Security – Data Centre

The CHSPOS SaaS infrastructure is hosted in a Tier – III data centre, which provides numerous controls and safeguards over customer data. We can share the Equinix technical documentation for the data centre upon request.

Our Cloud Service Provider has industry certification demonstrating best practises for physical and logical security of their Data Centre hosting environment. The Equinix Sydney data centre is compliant to the following industry standards.

- ISO 27001
- PCI DSS
- SOC 1 Type II
- SOC 2 Type II

Data Backup Policy

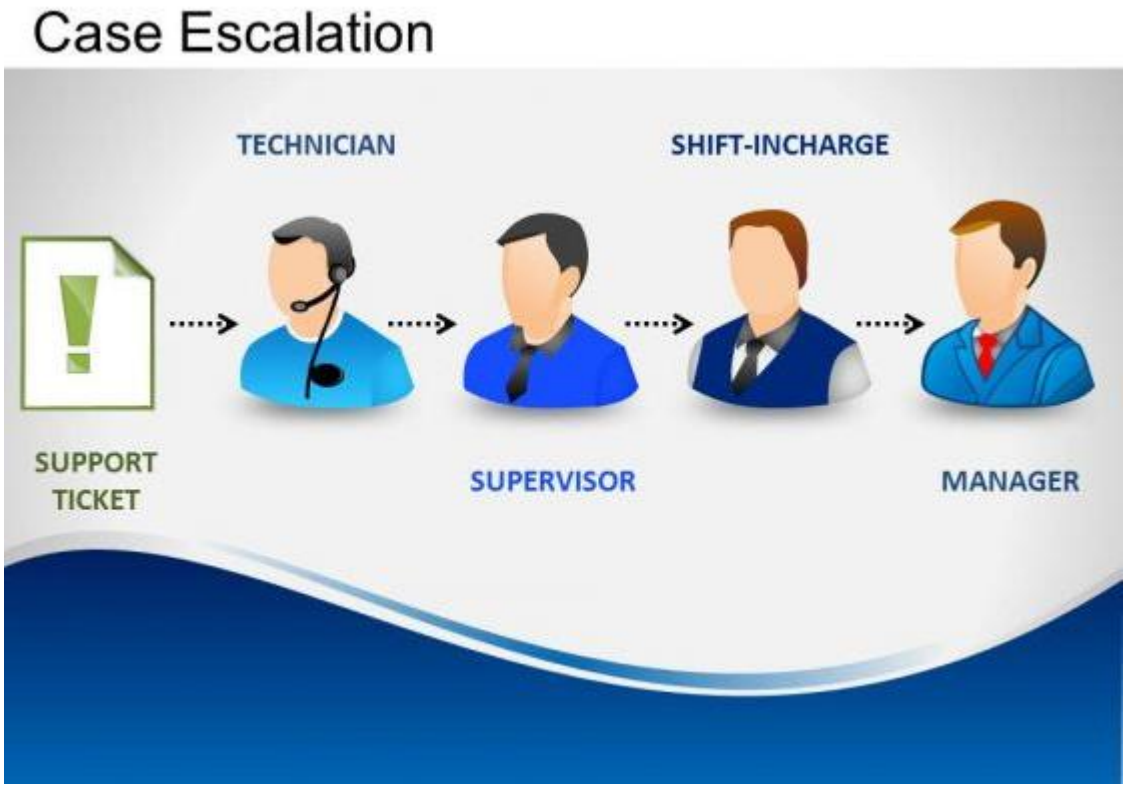
The CHSPOS SaaS Online backup policy is structured in the following hierarchy:

- Daily backups are kept for 14 days.
- Weekly backups are kept for 3 months.
- Monthly backups are kept for 12 months.
- We delete any backup greater than 12 months.

These backups enable us to restore the entire CHSPOS SaaS system. Our backups have the functionality for complete multiple backups for the entire SaaS environment, down to the granular point of each individual tenant's data store.

Support & Escalation process

CHSPOS support have a well defined and monitored incident handling system. Support is available between the hours of 6am to 11pm 7 days a week (EST) with an escalation process from level 1 support through to the CEO.



Data governance and privacy

Your data is your own. Only your authorised users have access to data stored in CHSPOS SaaS —CHSPOS employees only have access to your data with your consent other customers do not have access to your data. The only exception is a small and controlled number of CHSPOS system administrators who have access to the global system.

CHSPOS monitors metrics that have to do with system utilisation, account status, and performance. Such metrics include:

- Total storage used by account and by user.
- Total bandwidth used by account and by user.
- Access dates and times by user (logins).
- Site performance metrics.

Destruction of data

CHSPOS will destroy all data associated with your account if you request that we do so. Data contained in backups will be purged over time as part of regular backup purges. Purges are based on legislative compliance to Storage of Records Act.

Lifecycle management of our services

CHSPOS uses “Agile” as its product lifecycle management methodology, so all new features releases, change requests, support and maintenance calls are managed using SCRUM.

Operational processes

We also enforce through internal policies, including controls on how we manage the infrastructure and development of CHSPOS SaaS. Every CHSPOS employee undergoes a criminal and reference background check before joining the company.

User Security

Access and authentication

The only users that have access to your site content are those that you have explicitly added to the site. User management is completely in your control. If a user is no longer authorised in your system, simply remove them and they will no longer have access to content stored in CHSPOS SaaS.

Roles & permissions

In CHS, a role is a set of permissions that is applied to content to manage how users and groups can interact with objects such as modules and reports. Administrators can create groups such as “Employee Users” or “Head-Office Users” to make permission management easier. Roles provide a default permission structure to differentiate users. The typical actions of view, create, modify, and delete are implemented through the embedded web-portal interface and through the CSV import module.

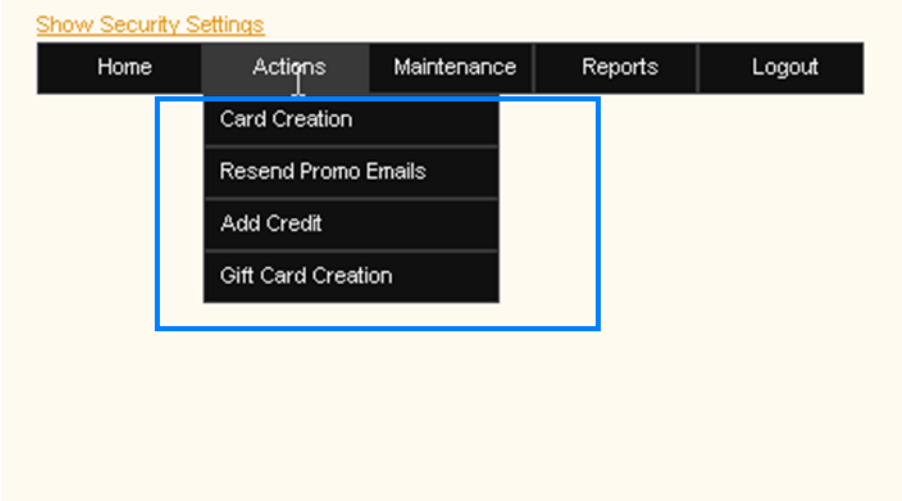
Data Security

Data enters the CHSPOS SaaS in one of following ways:

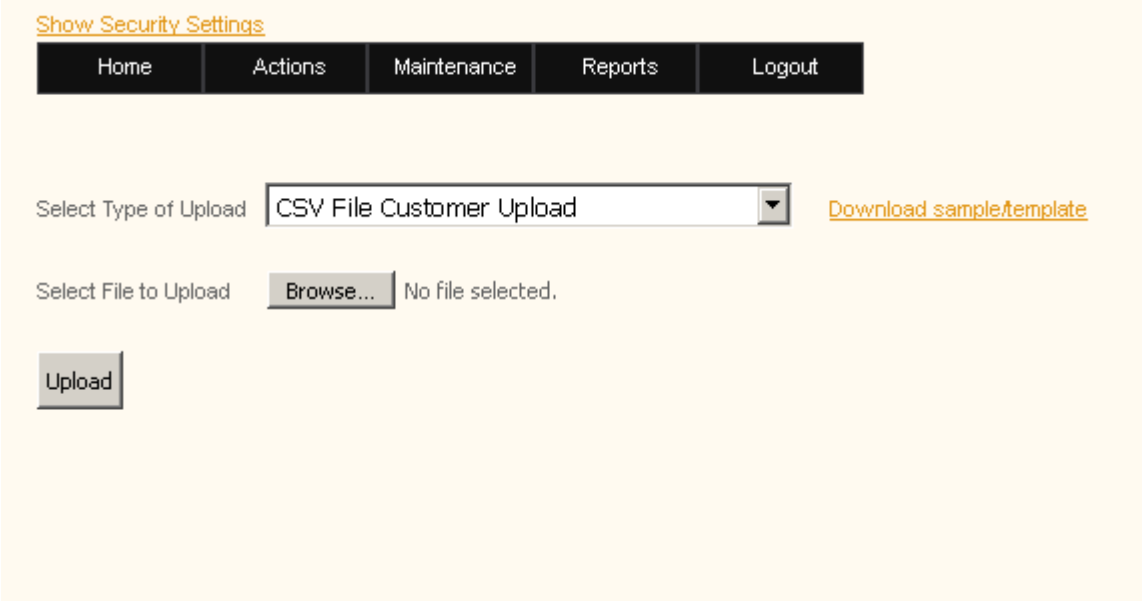
- By adding data using the embedded web portal menu options
- By bulk card detail updating via CSV file upload

Data Exchange - Bulk Credit Adjustments, Roles, and Reporting

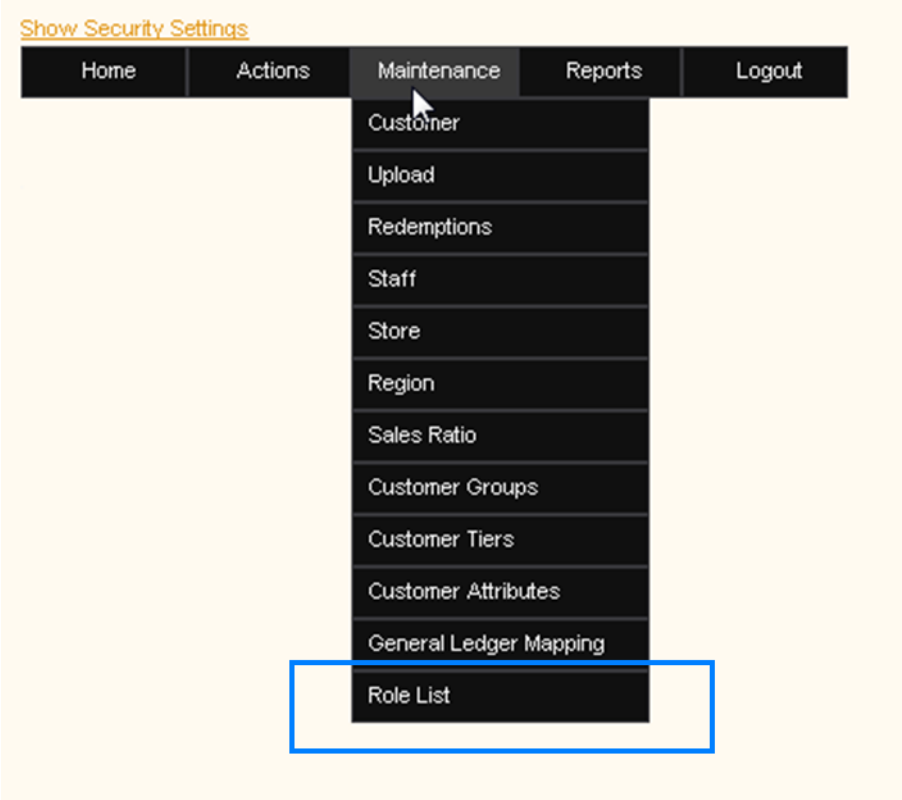
Creation of rewards cards via the embedded web portal



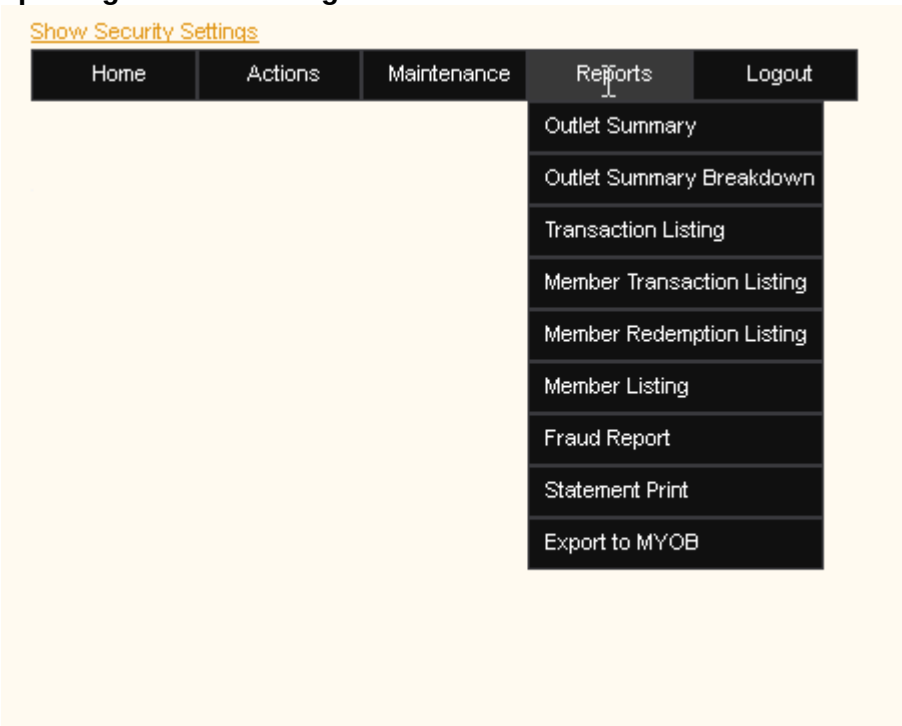
Bulk changes to card amounts and details via CSV file upload



Permissions & Roles



Reporting and Monitoring



Transmission (Network) Security

Encryption

All communication between you and CHSPOS SaaS is conducted using HTTPS / TLS for secure transmission of data, with the exception of subscription emails, which are clear text by Internet convention. In addition, CHSPOS SaaS has many built-in security mechanisms to help prevent spoofing, hi-jacking, and SQL injection attacks, and actively tests and responds to new threats with updates on a regular basis.

Application security

Application security is a combination of secure design practices and regular audits. We have worked with domain specialist to conduct a complete security audit of CHSPOS SaaS, including penetration testing, security testing and source code review. We will continue to work with third-party security experts to discover, test, address and validate any security concerns.

Multi-tenant architecture

The CHSPOS SaaS environment is hosted in a multi- tenant configuration providing partitioning of users, data, and metadata across customers. This means that a customer cannot access another customer's data. This includes the data itself, data about the data (metadata) like modules and data source names, as well as user names and groups. All of that is private to each customer.

Glossary

CSP	Cloud Service Provider
HTTPS	Hypertext Transfer Protocol Secure
IPSEC	Internet Protocol Security
SAAS	Software as a Service
TLS	Transport Layer Security
VM	Virtual Machine

Conclusion

CHSPOS SaaS has a robust security model as well as 24x7 monitoring. Security is of the highest priority for our customers, as it is for us aswell.

By

POSERA