ServicePattern PCI-DSS Compliance Features

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle payment cards from the major card brands. While the standard itself applies to entities involved in payment card processing, the technology solutions employed by such entities are expected facilitate compliance. Below is a summary of ServicePattern features that enable contact centers to be PCI-DSS compliant.

Infrastructure

ServicePattern supports multi-tier/zone operation for PCI-compliant enterprise and multi-tenant deployments. Tenants have access only to their own resources and the critical system level-functions can be firewalled independently. API access can be restricted to specific IP ranges. Each tenant has its own data encryption key that can be changed at any time and is protected by a key encryption key, which is stored separately.

Access Control

ServicePattern uses a role-based system to control access to specific contact center functions, where access to client data is protected by special privileges. All user accounts are password protected and password complexity rules can be enforced at the service provider level for all system- and tenant level accounts. Passwords are never displayed or stored in clear text. Accounts can be locked out after a pre-defined number of unsuccessful login attempts. Compromised accounts can be deactivated without losing any configuration or historical data associated with them. Inactive admin-level user sessions are terminated automatically.

Storage and Transmission of Sensitive Data

All data elements where cardholder information may appear can be encrypted for storage. This includes voice and screen recordings, email content, chat transcripts, as well as custom fields of calling lists and activity forms. Use of secure protocols can be enforced for all external interfaces involving transmission of this data. Logging of such data can also be completely disabled in production mode. To support the recent PCI requirement that prohibits storage of sensitive authentication data (PIN, CCV, etc.) in any form, voice recordings can be paused either manually by agents or by a third-party application via API for the duration of cardholder authentication. Cardholder authentication process can be delegated to an IVR application.

Audit Trail

Audit logs contain information about all login sessions including unsuccessful attempts. For successful logins, all admin-level operations are logged including the date/time, type of operation, and affected resources. Access to audit log is protected by a dedicated privilege. Audit trail can be stored in a PCI-compliant manner (at least one year with immediate access to at least last three months).

Specification

Infrastructure

- multi-tier/zone operation support
- separation of system and tenant-level functions
- independent firewalling of system-level functions
- cross site scripting (XSS) protection
- cross site request forgery (CSRF) protection
- per-tenant data encryption keys
- data encryption key protected by key encryption keys that is stored separately
- data encryption key can be changed at any time

Storage and Transmission of Sensitive Data

- encryption of all data elements where sensitive data may appear
- use of secure protocols for all external interfaces (SSL/TLS, HTTPS, SFTP)
- rendering sensitive data unreadable in logs
- pausing voice recording from agent desktop
- pausing voice recording via API
- support for out-of-band DTMF (RFC 2833/4733)
- delegating cardholder authentication to IVR

Access Control

- password-protected user accounts
- password complexity rules enforceable at service provider level
- password encryption/masking
- account lock-out with configurable number of unsuccessful login attempts
- account deactivation without loss of configuration or historical data
- forced log-out of inactive user sessions
- role-based access control system
- dedicated privileges for access to sensitive client data

Audit trail

- system-level and tenant-level audit logs
- information about all login sessions including unsuccessful login attempts
- logging of all admin-level operations
- complete log record (timestamp, user, operation type, and affected resource)
- access to audit log protected by a dedicated privilege
- configurable audit trail storage time