# UCSC Security Policy Template, SAQ P2PE V 4.0

## *Requirement 3:*

## *Protect Stored Account Data*

Note: For SAQ P2PE, Requirement 3 applies only to merchants with paper records that include account data (for example, receipts or printed reports).

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.1.1 All security policies and operational procedures that are identified in Requirement 3 are:

* Documented.
* Kept up to date.
* In use.
* Known to all affected parties.

3.2 Storage of account data is kept to a minimum.

3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:

* Coverage for all locations of stored account data.
* Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization
* Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
* Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
* Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
* A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

3.3.1.2 The card verification code is not retained upon completion of the authorization process

## *Requirement 9:*

## *Restrict Physical Access to Cardholder Data*

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

9.1.1 All security policies and operational procedures that are identified in Requirement 9 are:

* Documented.
* Kept up to date.
* In use.
* Known to all affected parties.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

*Note: For SAQ P2PE, Requirements at 9.4 only apply to merchants with paper records (for example, receipts or printed reports) with account data, including primary account numbers (PANs).*

9.4.1 All media with cardholder data is physically secured.

9.4.1.1 Offline media backups with cardholder data are stored in a secure location.

9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:

* Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
* Materials are stored in secure storage containers prior to destruction.

9.5Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

* Maintaining a list of POI devices.
* Periodically inspecting POI devices to look for tampering or unauthorized substitution.
* Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

9.5.1.1An up-to-date list of POI devices is maintained, including:

* Make and model of the device.
* Location of device.
* Device serial number or other methods of unique identification.

9.5.1.2POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

9.5.1.3Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:

* Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
* Procedures to ensure devices are not installed, replaced, or returned without verification.
* Being aware of suspicious behavior around devices.
* Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

## *Requirement 12*

## *Support Information Security with Organizational Policies and Programs*

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current.

12.1.1 An overall information security policy is:

* Established.
* Published.
* Maintained.
* Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

12.1.2 The information security policy is:

* Reviewed at least once every 12 months.
* Updated as needed to reflect changes to business objectives or risks to the environment

12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.

12.6 Security awareness education is an ongoing activity.

12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity’s information security policy and procedures, and their role in protecting the cardholder data.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

12.8.2 Written agreements with TPSPs are maintained as follows:

* Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
* Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity’s CDE.

12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

12.8.4 A program is implemented to monitor TPSPs’ PCI DSS compliance status at least once every 12 months.

12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident.

**Incident Response Plan**

This template is general, and must be updated to apply to your specific merchant operation. Please contact the Campus PCI Coordinator for assistance in customizing your plan.

To guide the response to an incident, the following team has been assigned specific responsibilities:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Role** | **Contact Details** | **Duties** |
| [FILL IN] | Departmental PCI Coordinator | [FILL IN] | Inform UCSC PCI Coordinator and departmental staff |
| Scott Morley | Campus PCI Coordinator | merchantservices@ucsc.edu | Inform all appropriate parties, including ITS/Core-Tech, UCPD, and Bank if necessary |
| [FILL IN] | Department Head | [FILL IN] | Assist Departmental PCI Coordinator with resources to accomplish resolution of incident |

For Card-Present Breaches

If a terminal device shows evidence of tampering, is missing or stolen, the departmental PCI Coordinator or Department head will immediately notify Campus PCI Coordinator by email using the contact information above. Isolate the machine and ensure that no further credit card transactions are run on it until it is inspected by the Campus PCI Coordinator.