# UCSC Security Policy Template, SAQ A V 4.0

## *Requirement 2:*

## *Apply Secure Configurations to All System Components*

2.2.2 Vendor default accounts are managed as follows:

* If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
* If the vendor default account(s) will not be used, the account is removed or disabled.

## *Requirement 3:*

## *Protect Stored Account Data*

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.

Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted.

## *Requirement 6*

## *Develop and Maintain Secure Systems and Software*

6.3 Security vulnerabilities are identified and addressed.

6.3.1 Security vulnerabilities are identified and managed as follows:

* New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
* Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
* Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.

6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

* Critical or high-security patches/updates are installed within one month of release.

6.4 Public-facing web applications are protected against attacks.

**Note:** *For SAQ A, Requirement 6.4.3 applies to a merchant’s website(s) that includes a TPSP’s/payment processor’s embedded payment page/form (for example, an inline frame or iFrame).*

6.4.3 All payment page scripts that are loaded and executed in the consumer’s browser are managed as follows:

* A method is implemented to confirm that each script is authorized.
* A method is implemented to assure the integrity of each script.
* An inventory of all scripts is maintained with written justification as to why each is necessary.

**Note:** This requirement applies to all scripts loaded from the entity’s environment and scripts loaded from third and fourth parties.

## *Requirement 8:*

## *Identify Users and Authenticate Access to System Components*

**Note:** *For SAQ A, Requirement 8 applies to merchant webservers that host the page(s) that either 1) redirects customers from the merchant website to a TPSP/payment processor for payment processing (for example, with a URL redirect) or 2) includes a TPSP’s/payment processor’s embedded payment page/form (for example, an inline frame or iFrame).*

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account’s lifecycle

8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.

Note: This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:

* Account use is prevented unless needed for an exceptional circumstance.
* Use is limited to the time needed for the exceptional circumstance.
* Business justification for use is documented.
* Use is explicitly approved by management.
* Individual user identity is confirmed before access to an account is granted.
* Every action taken is attributable to an individual user.

8.2.5 Access for terminated users is immediately revoked.

8.3 Strong authentication for users and administrators is established and managed.

8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:

* Something you know, such as a password or passphrase.
* Something you have, such as a token device or smart card.
* Something you are, such as a biometric element.

8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:

* Set to a unique value for first-time use and upon reset.
* Forced to be changed immediately after the first use.

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

* A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
* Contain both numeric and alphabetic characters.

8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:

* Passwords/passphrases are changed at least once every 90 days,
* **OR** The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly

## *Requirement 9:*

## *Restrict Physical Access to Cardholder Data*

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

Note: For SAQ A, 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.

9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.

9.4.3 Media with cardholder data sent outside the facility is secured as follows:

* Media is sent by secured courier or other delivery method that can be accurately tracked.

9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).

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.

## *Requirement 11:*

## *Test Security of Systems and Networks Regularly*

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.3.2 External vulnerability scans are performed as follows:

* At least once every three months.
* By PCI SSC Approved Scanning Vendor (ASV).
* Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
* Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.

11.3.2.1 External vulnerability scans are performed after any significant change as follows:

* Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
* Rescans are conducted as needed.
* Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV)

11.6 Unauthorized changes on payment pages are detected and responded to.

**Note:** *For SAQ A, Requirement 11.6.1 applies to a merchant’s website that includes a TPSP’s/payment processor’s embedded payment page/form (for example, an inline frame or iFrame).*

11.6.1 A change- and tamper-detection mechanism is deployed as follows:

* To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
* The mechanism is configured to evaluate the received HTTP header and payment page.
* The mechanism functions are performed as follows:
	+ At least once every seven days **OR**
	+ Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).

## *Requirement 12:*

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

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. The plan includes, but is not limited to:

* Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
* Incident response procedures with specific containment and mitigation activities for different types of incidents.
* Business recovery and continuity procedures.
* Data backup processes.
* Analysis of legal requirements for reporting compromises.
* Coverage and responses of all critical system components.
* Reference or inclusion of incident response procedures from the payment brands.

**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 E-Commerce Breaches:

A breach alert may come from your third party service provider, or a customer informing your office about fraud on their card that could only have come from your office. If anyone in your department is informed of a breach, your departmental PCI Coordinator or Department head will immediately notify Campus PCI Coordinator by email using the contact information above.

The Campus PCI Coordinator will work with you and your vendor to confirm if a breach has occurred. In the event that one has occurred, the platform will be shut down while an investigation takes place. Campus PCI Coordinator will inform the UCSC CISO, and the merchant will work with their vendor and the Campus PCI Coordinator to inform customers of the breach. This is typically handled by the third party service provider. UCSC PCI Coordinator will also inform the acquiring bank as appropriate.

Following this, UCSC’s CISO will advise on next steps.