PAYMENT CARD INDUSTRY DATA SECURITY

I. POLICY

Salt Lake Community College complies with established Payment Card Industry Data Security Standards (PCI DSS) when accepting payments by payment card. PCI DSS standards include requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The following procedures establish internal controls for maintaining these standards.

II. REFERENCES

Payment Card Industry Security Council – Current Data Security Standards.

III. DEFINITIONS

A. **Cardholder Data (CHD):** data that contains the full card account number, expiration date, and cardholder name.

B. **Information Security Office (ISO):** an office within the Office of Information Technology responsible for the security of sensitive data. ISO employees are designated as information security officers and assist college departments, safeguard data systems, and otherwise comply with data security standards and practices.

C. **Payment Card:** a bank-issued debit or credit card (e.g., Visa, MasterCard, American Express, or Discover) and the college One-Card, including contactless payment apps such as Apple Pay.

D. **Payment Card Industry Data Security Standards (PCI DSS):** standards established by the Payment Card Industry Security Standards Council. Any business or organization that accepts payment cards must comply with these standards.

E. **Payment Card Industry Security Team (PCI Team):** a group of college employees responsible for compliance with payment card industry data security standards.

IV. PROCEDURES

A. General Procedures

1. The college strictly forbids the storage of sensitive authentication data including the contents of the magnetic stripe, the card validation or security code and PIN, or block.

2. The college prohibits the storage of cardholder data (CHD).
3. Employees must not transmit CHD without an approved PCI policy compliant device or technology.
4. OIT is responsible for maintaining secure college networks, systems, and applications involving payment card transactions and monitoring and testing systems following the PCI data security standards.
5. Vendors must provide documentation that the system or device complies with current PCI standards before a college department is authorized to use a service provider or third-party point-of-sale software system that accepts payment cards or uses a vendor's credit card reader device,
6. Documentation must be submitted to the ISO before the system or device is used.
7. Employees must report a suspected data security breach immediately to the PCI Team. The team is responsible for investigating and informing the vice president for Finance and Administration of any potential or confirmed data breaches.

B. PCI Security Team

1. The college must establish a PCI Team comprising, at minimum, a representative from the Controller's Office, the Chief Information Security Officer (CISO), the Information Security Officer (ISO), and bursar or bursar's designee.
2. The team will be exclusively responsible for:
    a. implementing a security awareness program to educate all employees regarding the importance of cardholder data security;
    b. establishing, documenting and distributing security procedures and related updates;
    c. monitoring ongoing security compliance and making updates to the procedures as the environment changes;
    d. providing input and grant approval for the adoption of or changes in critical information technologies that could impact data security;
    e. being first responders in the event of a system breach; and analyzing security alerts, documenting, and coordinating security incident responses to ensure situations are handled in a timely and effective manner.

C. PCI Data Security Procedures

1. Network Diagrams
    a. OIT will create and access network diagrams.
    b. Network diagrams must be reviewed by OIT when there is a system change and at least annually to ensure that CHD is secure.

c. Current, accurate network diagrams should be maintained by OIT to ensure that all the appropriate firewalls and segmentation are enforced.

2. Third Party Software

   a. College departments that use third-party software must ensure that CHD is secure at every point as it is transmitted across college networks to outside networks.

   b. Any changes that occur with third-party software upgrades, changes in college devices, or relocation of college devices, must be documented by the bursar's office immediately.

3. Password Protection and Vendor Defaults

   a. College system administrators and the bursar's office payment system specialist must always change, remove, or disable vendor-supplied defaults or accounts before installing the following on the college network:

      (1) operating systems;

      (2) software that provides security services;

      (3) point-of-sale devices and terminals; and

      (4) third-party payment application data security standard (PA-DSS) software.

   b. Wireless Networks (Wi-Fi)

      College departments must not use the college's wireless network for any PCI system that processes or transmits CHD.

4. System-hardening

   All PCI system components must be configured according to industry-accepted system-hardening standards including:

   a. Center for Internet Security (CIS);

   b. International Organization for Standardization (ISO); and

   c. National Institute of Standards Technology (NIST).

5. Approved Devices

   a. The bursar's office must approve all devices used to process CHD.

   b. Only mobile devices approved by the bursar's office can be used to process CHD.

   c. All mobile devices must have an automatic disconnect of the session after a designated period of inactivity, usually 30 minutes.

d. Single Purpose Devices

(1) PCI devices such as desktops, web servers, database servers, and DNS servers must be configured by OIT to prevent operations that require different security levels from co-existing on the same device.

(2) Desktops with card processing software or web access to a third-party vendor must not have other programs or web-surfing capabilities. Only necessary services, protocols, daemons, etc. required for the system's function will be enabled.

6. Secure Cryptography and Transport Layer Security (TLS)

a. Additional security features for required services, protocols, or daemons, such as NetBIOS, file-sharing, Telnet, file transfer protocol (FTP), etc., must be secured with the most recent version of TLS.

b. Secure shell (SSH), secure file transfer protocol (S-FTP), or internet protocol security virtual private network (IPsec VPN) are also allowed.

c. Secure sockets layer (SSL) is not secure encryption.

7. Preventing System Misuse

a. All college systems components will have only the necessary configuration to support payment processing functionality.

b. All unnecessary functions must be removed by OIT to prevent misuse and reduce risk to the PCI environment.

8. Maintain System Component Inventory

The bursar will keep an inventory of all PCI devices and components, including:

a. hardware serial numbers, model names, and locations;

b. IP addresses, DNS, VLANs, and operating systems;

c. the purpose of the components; and

d. the owners.

9. CHD Retention and Storage

a. CHD on Paper

(1) CHD taken by phone for payments must be processed immediately.

(2) Only the cardholder's name, address, card number, and expiration date should be put on paper.

(3) Once processed, the paper containing the CHD should be immediately destroyed using a crosscut shredder.

(4) The college forbids any other form of storage and acceptance of CHD by facsimile (fax) or email.

b. Sensitive CHD

(1) All department points of contact shall sign an annual document which states they are not storing sensitive data.

(2) Sensitive authentication data, including CVV or CVC, PIN or PIN blocks, or full track data (from a magnetic stripe or a chip), must never be stored.

c. CHD should never be recorded or stored anywhere digitally or physically including removable media or spreadsheets.

10. Encrypt Transmission of CHD Across Open, Public Networks

a. Strong cryptography and security protocols must be used to safeguard CHD during transmission over open, public networks.

b. OIT only accepts trusted keys or certificates and employs industry best practices to implement strong encryption for wireless networks authenticating and transmitting CHD or connected to the CHD environment.

11. Vulnerability Management

a. The college uses anti-virus software on all applicable PCI devices, including those system types that are most affected by malicious software.

b. OIT regularly evaluates all systems with anti-virus to ensure they can remove malware threats.

12. Maintaining Anti-virus Mechanisms

OIT updates anti-virus software to ensure that the anti-virus:

a. is kept current;

b. can be scanned;

c. can be logged as per PCI DSS Requirement 10.7.; and

d. has not been removed, altered, or disabled.

13. Change Control Procedures

a. To make changes to PCI equipment, departments must complete a request for change through the bursar's office and include all applicable documentation.

b. When a security patch is applied, or there are software modifications, OIT and the bursar's office must coordinate to document and permanently retain:

(1) the impact of the change; and

(2) the approvals that are required from all parties.

c. For any changes, the vendor must provide documentation to prove a PCI assessment that shows compliance after the change was made.

d. All documentation changes should be sent to the bursar.

14. Access Controls

a. The college assigns a unique ID to each person with computer access.

b. Only personnel with a legitimate business need may access CHD or other sensitive data.

c. The bursar's office must create a list of roles according to the position and duties of an employee.

(1) The bursar's office must assign and document the level of access to each role.

(2) The bursar's office must assign each employee the least amount of privileges necessary to perform their duties.

d. For automated systems and manual processes, access controls must be implemented by the bursar's office as soon as they are created.

(1) Every component must have the required access controls implemented.

(2) Department documentation must include:

i. dates of creation and implementation of each access control;

ii. each component that requires access control; and

iii. a description of the access, which roles need the access, and the position within the role.

(3) Users must be informed regarding their degree of access and the required security responsibilities.

(4) Roles for access controls shall be reviewed when changes are made and at least annually.

(5) The bursar's office must approve documentation.

(6) All access control documentation shall be completed and maintained within the bursar's office.

e. Departments will have risk assessments performed annually.

15. Regularly Monitor and Test Networks

OIT will:

a. monitor and test networks;

b. perform audits of individual access to CHD; and

c. implement an audit trail.

16. Regular Testing of Security Systems and Processes

a. Internal and External Network Vulnerability Scans

(1) OIT will scan all third-party software system components or desktop computers that access a third-party vendor's hosted web service for processing payment cards weekly.

(2) Any discovered vulnerabilities will be remediated within 30 days.

(3) Scans will be rerun until all high-risk vulnerabilities are resolved.

(4) OIT must perform internal scans as patches and updates are made to their CHD environment.

(5) External Network Vulnerability Scans will be run quarterly on all public facing PCI systems.

b. Penetration Testing

(1) A qualified internal or external entity designated by OIT will perform penetration testing on the applicable PCI systems.

(2) OIT will ensure that the designated entity uses testing methodology outlined in PCI DSS Requirement 11.3.

(3) Penetration testing will be completed by OIT whenever system changes have been made to the PCI environment and at least annually.

(4) System changes are defined as well documented, low risk, and proven

(5) Standard changes are done regularly according to industry best practice recommendations.

(6) Instances of a standard change to 'primary systems' need to be submitted to and reviewed by OIT through Change Control Team Meeting before implementation.

(7) Instances of a standard change to 'non-primary systems' need to be submitted to and reviewed by OIT through Change Control Team Meeting before implementation.

(8) Coordination activities can be done at the discretion of the Information Security Office.

c. Change Classifications

(1) Minor Change: a change that has a low impact on the number of users affected or the service's criticality, a low risk of failure, and a required lead-time with change notification made through standard methods

i. Minor changes are reviewed at the Change Control Team Meeting and approved by OIT.

ii. Coordination activities can be done at the discretion of the Information Security Office.

(2) Major Change: a change that has a significant impact on users or services, a high risk of failure, or is complex and requires multiple teams to implement. This change may also include new, high-profile applications used in production for the first time or changes to applications requiring a high degree of coordination between multiple organizations.

i. Coordination activities can be done at the discretion of all the groups/individuals involved.

(3) Emergency Change: a change that must occur immediately to fix severe loss in service capability.

i. Communication and updates will be performed through standard notification methods.

(4) Significant Change: a change that may include standard, minor, major, or emergency changes and is highly dependent on the configuration of a given environment.

i. If an upgrade or modification could allow access to CHD or affect the security of the CHD environment, then it could be considered significant. Refer to Significant Change Requirements.

d. Intrusion Detection

(1) OIT monitors all traffic and notifies departments of any suspected threats or compromises.

(2) Departments must respond immediately following notification of a suspected threat or compromise.

e. Change Detection

(1) College-approved endpoint protection software must be used on all systems using third-party vendors to detect changes, additions, and deletions of critical system files, configuration files, or content files, including operating system programs and application executables.

(2) OIT monitors endpoint protection for alerts and unauthorized changes.

(3) When the third-party vendor does not support college-approved endpoint protection, documentation must be provided from the vendor that the system is security hardened and meets OIT requirements.

17. Daily Operational Security Procedures

    a. Each department must maintain daily operational procedures to ensure that its operations are secure and meet each PCI Standard.

    b. Security procedures must:

        (1) include all technical and administrative functions;

        (2) be in place, and logs should be kept for user account additions, changes, and deletions.;

        (3) be reviewed by employees at least annually.

    c. The bursar's office and OIT must date, document, and maintain any system changes or incidents.

18. Usage Policies and Procedures

    a. OIT implements procedures that secure usage of remote access technologies, wireless technologies, removable electronic media, laptops, tablets, PDS's, email, fax, and internet.

    b. OIT's Procedures require, and departments must enforce, any third-party software or CHD system be authenticated by a user ID and password and two-factor authentication.

    c. OIT's Procedures include formal written authorization approving access to each CHD technology and documentation listing all devices and the employees that use each device.

    d. Documentation must be kept and updated.

    e. Vendors and third parties may have limited access to college systems.

        (1) Prior arrangements should be made to allow access.

        (2) Access should be granted for only the required amount of time.

        (3) Departments must require the vendor or third party to use the college's two-factor authentication solution.

        (4) The college must ensure through internal procedures that employees are informed that no CHD is be copied, moved, or stored on local hard drives and removable electronic media.

19. Security Responsibilities for Personnel

    a. Security for each responsibility must be defined and distributed to employees.

b. Documentation demonstrating that each employee understands their security responsibility shall be maintained and updated by the department.

20. Assignment of Security Management Responsibilities

    a. The chief information security officer and the PCI Team share the responsibility of security management.

    b. The chief information security officer is responsible for establishing, documenting, and distributing security incident responses.

    c. The PCI Team is responsible for:

        (1) establishing, documenting, and distributing security policies and procedures;

        (2) suggesting policy updates when there is a change in procedure; and

        (3) creating, maintaining, and executing escalation procedures and processes.

    d. Departments are responsible for:

        (1) monitoring and controlling access to data;

        (2) administering, adding, deleting, and modifying user access, and informing the bursar; and

        (3) distributing security incident procedures to employees.

21. Formal Security Awareness Program

    a. OIT provides formal training for every employee who has access to CHD.

    b. Departments must provide a list of employees with CHD access at least annually or when there is a new hire, change in duties, or termination.

    c. The bursar will send a notification to an employee when it is time for that employee's annual training.

    d. The bursar will maintain a database of employees authorized to access CHD and update it as employees complete training.

    e. The bursar will email updates to PCI information or changes in procedures to the employees in the database.

22. Background Checks

    PCI DDS standards require background checks are performed on all college employees who have access to CHD.

23. Incident Response Plan

a. Departments must maintain an internal incident response plan to report incidents to the Controller's Office and the chief information security officer.

b. Anyone who identifies an incident must immediately report it to the department manager or director.

c. The director or manager must document events in a report and forward the report to the Controller's Office and the chief information security officer. The report must include:

    (1) the date incident was found;

    (2) the type of incident;

    (3) how the department became aware of the incident; and

    (4) whether or not the department disabled the breached device or system.