CARDHOLDER DATA INFORMATION SECURITY POLICY

This policy is intended to relay the importance of security and protecting cardholder data and to establish the Sequoias Community College District policy for the secure handling of sensitive card holder data including but not limited to magnetic strip data, Primary Account Numbers (PAN's), expiration date, and service code. This policy applies to all employees and systems of the District who collect/accept cardholder data.

Policies to Protect and Manage Cardholder Data

The importance of protecting cardholder data is paramount. Allowing data theft or destruction, inadvertently sharing confidential information, infecting system networks with viruses, misuse of company resources, allowing the theft of company property, and allowing the compromise of private or confidential company or client information are all very real examples of what might result from a security compromise.

1. All sending of unencrypted Primary Account Numbers by end-user messaging technologies (i.e., email, instant messaging, and chat) are strictly prohibited. If a PAN must be sent by end-user messaging, only email is allowed and the PAN will be encrypted using WinZip. The WinZip password will be communicated to the end user by means other than end user messaging (phone or fax is allowed).

2. Access to system components and cardholder data is limited to only those authorized individuals whose job require such access or have a need-to-know. This authority is granted by senior management and reviewed annually.

3. All paper that contains cardholder data is to be identified and physically secured in a locked drawer. No electronic cardholder data will ever be stored.

4. Strict control is to be maintained over the internal or external distribution of any kind of media that contains cardholder data.
    a. Media is classified and clearly marked as confidential
    b. Media is sent by secured courier or other delivery method that can be accurately tracked.

5. Management approval is to be obtained prior to moving any and all media containing cardholder data from a secured area.

6. Strict control must be maintained over the storage and accessibility of media that contains cardholder data.
7. Media containing cardholder data is to be destroyed when it is no longer needed for business or legal reasons.
    a. Paper materials are to be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.

b. The general rule is that media containing cardholder data will be destroyed when over 180 days old. Exceptions to the rule must be approved by Fiscal Services.

Policy Maintenance and Employee/Contractor Awareness

1. Review of this policy will be conducted on an annual basis or as changes to the environment occur.

2. Usage of employee-facing technologies such as remote access, wireless, electronic media, internet, PDA's and wireless will adhere to the following:
   a. No unauthorized equipment can be brought in or set up in the College facility. This includes, but is not limited to modems, computers, or wireless devices.
   b. Wireless devices must be set up securely by establishing secure accounts/passwords, disabling SSID broadcasts, and using the highest available encryption for the device.

3. One or more employees will be designated with security responsibility.

4. Incident response documents will be created, reviewed by all employees, and will be updated on an annual basis.

5. These security policies will be formally reviewed annually with all employees/contractors.

6. A list of Service Providers must be maintained. This list will be updated and reviewed by Fiscal Services when necessary but at least every 180 days.

7. A written Agreement is required from each Service Provider that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider possesses is required from each Service Provider.

8. Due diligence is to be performed prior to the engagement of Service Providers. Procedures performed will include when possible:
   a. A written statement acknowledging their responsibilities to securely process, handle and transmit cardholder data.
   b. Written proof that the Service provider is PCI compliant.
   c. Request reliable industry references.

9. A program is to be maintained to monitor Service Providers' PCI DSS compliance status. On an annual basis a request for a new compliance certificate will be requested.

Adopted: May 9, 2011
Revised: January 8, 2018