SUNY SCHENECTADY COUNTY COMMUNITY COLLEGE

Financial

Board of Trustees Policy

SUBJECT:	NUMBER:
Payment Card Industry Data Security Standard Policy	6.7
	DATE: **March 18, 2024** **Resolution #24-08**
	SUPERSEDES: **July 20, 2015** **Resolution #15-75**

This policy document directly relates to the Payment Card Industry Data Security Standard Policy, of the SUNY Schenectady Board of Trustees, as hereto attached.

Contents

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential College information and must be distributed to all College employees. All College employees that handle PCI Data must read this document in its entirety and are required to take annual trainings to certify compliance with this policy. This document will be reviewed and updated by Financial Services and Information Technology Services on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contractors as applicable with the approval of the Board of Trustees.

2. Information Security Policy

The College handles sensitive cardholder information daily. Sensitive information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organization.

The College commits to respecting the privacy of all its students, customers, and users and protect any data about them from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data should ensure the following:

1. Handle-College and cardholder information in a manner that fits with their sensitivity;
2. Limit personal use of the College information and telecommunication systems and ensure it doesn't interfere with your job performance;
3. Do not disclose personnel information unless authorized;
4. Protect sensitive cardholder information;
5. Keep passwords and accounts secure;
6. Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
7. Do not install unauthorized software or hardware, including modems and wireless access unless you have explicit management approval;
8. Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
9. Information security incidents must be reported, without delay, to the Chief Information Officer for incident response locally.

We each have a responsibility for ensuring our College's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your department head or supervisor.

3. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee may result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for noncompliance.

4. Protect Stored Data

- All sensitive cardholder data stored and handled by the College and its employees must be securely protected against unauthorized use at all times. Any sensitive card data that is no longer required by the College for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see a card's full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger, email etc.,

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) on any media whatsoever.
2. The CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN Block under any circumstance.

5. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level.

- **Confidential data** might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to the College if disclosed or modified. **Confidential data includes cardholder data**.
- **Internal use data** might include information that the data owner feels should be protected to prevent unauthorized disclosure.
- **Public data** is information that may be freely disseminated.

6. Access to the Sensitive Cardholder Data

All access to sensitive cardholder should be controlled and authorized. Any job functions that require access to cardholder data should be clearly defined.

- Any display of the card holder data should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data.
- Access rights to privileged user ID's should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (role-based access control)
- Access to sensitive cardholder information such as PAN's, personal information and business data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this confidential data unless they have a genuine business need.
- If cardholder data is shared with a Service Provider (third party) then a list of such Service Providers will be maintained as detailed in Appendix A.
- The College will ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the cardholder data that the Service Provider possess.
- The College will ensure that a there is an established process, including proper due diligence, in place before engaging with a Service provider.
- The College will have a process in place to monitor the PCI DSS compliance status of the Service Provider.

7. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorized access to confidential data which includes card holder data.
- Employees should ensure that technologies should be used and setup in acceptable network locations.

- The Department of Financial Services will maintain a list of devices that accept payment card data.
    - The list should include make, model and location of the device.
    - The list should have the serial number or a unique identifier of the device.
    - The list should be updated when devices are added, removed or relocated.
- POS device surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices should be trained and aware of handling the POS devices.
- Personnel using the devices should verify the identity of any third-party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices.
- Personnel using the devices should be trained to report suspicious behavior and indications of tampering of the devices to the appropriate personnel.
- A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, USB drives, back-up tapes, computer hard drive, etc.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Media containing sensitive cardholder information must be stored in a secure, locked area while it is still required for use by the college.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, and consultants who are "resident" on the College sites. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- All network jacks used for POS and PIN entry should be isolated on a secure VLan.
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing card holder data and has to be approved by management
- Strict control is maintained over the storage and accessibility of media
- All computers that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorized use.

8. Protect Data in Transit

- All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.
- Card holder data (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorized by management, logged and inventoried before leaving the premises. Only secure courier services may be

used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

9. Disposal of Stored Data

- All data must be securely disposed of when no longer required by the College, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of cardholder data must be manually destroyed as when no longer required for valid and justified business reasons. The College will only keep the prior and the current semester's data. All other data is destroyed in January, May, and December of each year.
- The College will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The College will have documented procedures for the destruction of electronic media. These will require:
    - All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media;
    - If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

10. Security Awareness and Procedures

The policies and procedures outlined below must be followed to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all College employees that handle credit card information to read. It is required that all employees confirm that they understand the content of this security policy by completing and passing an annual Security Policy course provided by the College.
- All employees that handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the College.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- College security policies must be reviewed annually and updated as needed.

11. Remote Access policy

- It is the responsibility of the College employees, contractors, vendors and agents with remote access privileges to the College's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the College.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.

- Vendor accounts with access to the College network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be setup to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to the College internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or third parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification.
- Vendor accounts with access to the College network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

12. Vulnerability Management Policy

- All the vulnerabilities will be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
- As part of the PCI-DSS Compliance requirements, the College will run internal and external network vulnerability scans at least semi-annually and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Semi-annually internal vulnerability scans must be performed by the College by internal staff or a third-party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities, as defined in PCI DSS Requirement 6.2 of the Security Standards Council, are resolved.
- Semi-annually external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the College's internal staff. The scan process should include re-scans until passing results are obtained.

13. Audit and Log review

- This procedure covers all logs generated for systems within the cardholder data environment, based on the flow of cardholder data over the College's network, including the following components:

    1. Operating System Logs (Event Logs and SU (switch user) logs).
    2. Database Audit Logs.
    3. Firewalls & Network Switch Logs.
    4. IDS Logs.
    5. Antivirus Logs.
    6. CCTV Video recordings.
    7. File integrity monitoring system logs.

- Audit Logs must be maintained for a minimum of three months online (available for immediate analysis) and twelve months offline.

- Review of logs is to be carried out by means of the College's network monitoring system, which is controlled from the College console. The console is installed on the server, located within the College data centre environment.
- The following personnel are the only people permitted to access log files, Chief Information Officer (CIO), Information Security Officer or CIO delegated official.
- The network monitoring system software is configured to alert the College's IT Help Desk to any conditions deemed to be potentially suspicious, for further investigation. Alerts are configured to:

14. Incident Response Plan

'Security Incident' means any incident (accidental, intentional or deliberate) relating to your communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage your company.

The incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Employees of the College will be expected to report to the security officer for any security related issues.

The College PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to Chief Information Officer.
2. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and in mitigating the risks associated with the incident.
3. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
4. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
5. If an unauthorized wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Security Officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.
6. A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform the College PCI Incident Response Team. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments' response plans.

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure compromised system/s is isolated on/from the network.

2. Gather, review and analyse the logs and related information from various central and local safeguards and security controls.
3. Conduct appropriate forensic analysis of compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data.

Incident Response notifications to various card schemes:

1. In the event of a suspected security breach, alert the Information Security Officer or your line manager immediately.
2. The security officer will carry out an initial investigation of the suspected security breach.
3. Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps:

If the data security compromise involves credit card account numbers, implement the following procedure:

1. Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
2. Alert all affected parties and authorities such as the College's merchant bank services provider, Visa Fraud Control, and law enforcement.
3. Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
4. For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_ compromised.html

VISA Incident Report Template:

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and the College's merchant bank services provider. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
   a. Include overview of the incident.
   b. Include RISK Level (High, Medium, Low).
   c. Determine if compromise has been contained.

II. Background

III. Initial Analysis

IV. Investigative Procedures
   a. Include forensic tools used during investigation.

V. Findings
   a. Number of accounts at risk, identify those stores and compromised.
   b. Type of account information at risk.

c. Identify ALL systems analysed. Include the following:
    - Domain Name System (DNS) names.
    - Internet Protocol (IP) addresses.
    - Operating System (OS) version.
    - Function of system(s).

d. Identify ALL compromised systems. Include the following:
    - DNS names.
    - IP addresses.
    - OS version.
    - Function of System(s).

e. Timeframe of compromise.

f. Any data exported by intruder.

g. Establish how and source of compromise.

h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.).

i. If applicable, review VisaNet endpoint security and determine risk.

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

2. Distribute the account number data to its respective issuers.

Discover Card Steps:

1. Within 24 hours of an account compromise event, notify Discover Fraud Prevention.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from Discover Card.

American Express Steps:

1. Within 24 hours of an account compromise event, notify American Express Merchant Services.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
   Obtain additional specific requirements from American Express.

15. Roles and Responsibilities

The Chief Information Officer is responsible for overseeing all aspects of information security, including but not limited to:

1. Creating and distributing security policies and procedures.
   - Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.
2. Creating and distributing security incident response and escalation procedures that include:
   - Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
   - The Information Technology Office shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

System and Application Administrators shall:

1. Monitor and analyze security alerts and information and distribute to appropriate personnel.
2. Administer user accounts and manage authentication.
3. Monitor and control all access to data.
4. Maintain a list of service providers.
5. Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
6. Maintain a program to verify service providers' PCI-DSS compliant status, with supporting documentation.

The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

1. Facilitating participation upon hire and at least annually.
2. Ensuring that employees that handle PCI data acknowledge that they understand the College's PCI data policy by completing and passing a PCI data training course at least annually.

The Vice President of Administration, or his designee, and all parties involved will ensure that for service providers with whom cardholder information is shared:

1. Written contracts require adherence to PCI-DSS by the service provider.
2. Written contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.

Employees of the College will be expected to report to the Security Officer for any security related issues. The role of the Security Officer is to effectively communicate all security policies and procedures to employees within the College and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

16. Third party access to card holder data

- All third-party companies providing critical services to the College must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with the College's Physical Security and Access Control Policy.
- All third-party companies which have access to Card Holder information must:

    1. Adhere to the PCI DSS security requirements.
    2. Acknowledge their responsibility for securing the Card Holder data.
    3. Acknowledge that the Card Holder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
    4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
    5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.

17. Access Control Policy

- Access Control systems are in place to protect the interests of all users of the College computer systems by providing a safe, secure and readily accessible environment in which to work.
- The College will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.

- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services. Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the College CISO.
- Access to the College IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any the College IT resources and services will be provided without prior authentication and authorization of a user's the College Windows Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and expiration times will be controlled through Windows Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorized persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by the College policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, Windows share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, IIS intranet/extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users' access rights. The review shall be logged and IT Services shall sign off the review to give authority for users' continued access rights.

Appendix A

Asset/Device Name	Description	Owner/Approved User	Location	Service Provider
Square Card Reader	S/N 321LS17207111306 model S172	HCAT Department	Casola Dining Room	Square
iPad associated with Square Device	S/N DMPWPUBJF8K	HCAT Department	Casola Dining Room	Square
Square Register POS	S/N 309CS13A4000309 model CS130	HCAT Department	Pane e Dolci (HCAT)	Square
Square Customer Facing Display	S/N 307CP410A3000093 model CS131	HCAT Department	Pane e Dolci (HCAT)	Square
Square Card Reader	S/N 311CP378A1008124 model CP378	HCAT Department	Boucherie (HCAT)	Square
Square Card Reader	S/N 322CS149B3002991 model CS149	HCAT Department	Van Culer Room/Events (HCAT)	Square
Cellular Card Reader	S/N 009LS14602012187 model S146	HCAT Department	Food Truck (HCAT)	Square
VeriFone Model: Mx915	S/N 288-088-579	Bookstore (FSA)	Bookstore (FSA)	MBS
VeriFone Model: Mx915	S/N 288-088-578	Bookstore (FSA)	Bookstore (FSA)	MBS
VeriFone Model: Mx915	S/N288-088-498	Bookstore (FSA)	Bookstore (FSA)	MBS
VeriFone Model: Mx915	S/N 288-088-576	Bookstore (FSA)	Schwartz Café (FSA)	MBS
Clover Flex 2nd Generation	Model:K400 S/N C0426UQ91060303	SBO Department	SBO Department	Clover
Clover Flex 2nd Generation	Model:K400 S/N C043UQ201660478	SBO Department	SBO Department	Clover

Approved by the SUNY Schenectady Board of Trustees, March 18, 2024, Resolution # 24-08