IV:07:10 CREDIT CARD SECURITY POLICY

INTRODUCTION

The Payment Card Industry Data Security Standards (PCI DSS) is a set of comprehensive requirements for enhancing payment account and credit card data security. Please see https://www.pcisecuritystandards.org for additional information. Volunteer State Community College (VSCC) is committed to these security policies to protect information utilized by VSCC in serving our students, employees and constituents.

SCOPE OF COMPLIANCE

The PCI DSS requirements apply to all systems that store, process, or transmit cardholder data. Currently, VSCC's cardholder dataflow includes only paper media and that is only if necessary. Electronic storage of cardholder data is not conducted or permitted. Due to the limited nature of the in-scope environment, this document is intended to meet the PCI DSS requirements as defined in Self-Assessment Questionnaire (SAQ) C. Should VSCC implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of VSCC to determine the appropriate compliance criteria and implement additional policies and controls as needed. Other VSCC and TBR policies address information security and related matters such as TBR's policy 4-01-05-60 Identity Theft Prevention and VSCC's *Identity Theft Prevention Policy.* These policies should be considered in the interpretation and implementation of this policy.

Requirement 1: Build and Maintain a Secure Network

FIREWALL CONFIGURATION

VSCC will restrict firewall connections between un-trusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. (PCI Requirement 1.2)

VSCC firewalls will prohibit direct public access between the Internet and any system component in the cardholder data environment. (PCI requirement 1.3)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

VENDOR DEFAULTS

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Defaults for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to, default encryption keys, passwords and SNMP community strings. (PCI Requirement 2.1.1)

NON-CONSOLE ADMINISTRATIVE ACCESS

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. (PCI Requirement 2.3)

Requirement 3: Protect Stored Cardholder Data
PROHIBITED DATA

Sensitive authorization data will be retained only until completion of the authorization of a transaction. Storage of sensitive authorization data post-authorization is forbidden. Specifically, sensitive authorization data includes the following:

1. The full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. (PCI requirement 3.2.1)
2. The card verification code or value (three- or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. (PCI requirement 3.2.2)
3. The personal identification number (PIN) or the encrypted PIN block. (PCI requirement 3.2.3)

DISPLAYING PRIMARY ACCOUNT NUMBERS (PAN)

VSCC will mask the display of PANs, and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

TRANSMISSION OF CARDHOLDER DATA

VSCC will send cardholder data across open, public networks protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). (PCI Requirement 4.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: Use and Regularly Update Anti-Virus Software or Programs

ANTI-VIRUS

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

All anti-virus programs must be kept current, be actively running, and capable of generating audit logs within the PCI network. (PCI Requirement 5.2)

Requirement 6: Develop and Maintain Secure Systems and Applications

SECURITY PATCHES

All critical security patches must be installed within one month of release. (PCI Requirement 6.1)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

LIMIT ACCESS TO CARDHOLDER DATA

Access to VSCC's cardholder data is limited to only those individuals whose job requires such access. (PCI requirement 7.1)

Access limitations must include the following:

1. Restriction of access rights to cardholder data to the least access needed to perform job responsibilities.
2. Access to cardholder data is based on an individual's job classification and function.
3. Access to cardholder data within the computer system will be granted only after the approval of the required authorization request forms by the appropriate personnel.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

VENDOR ACCOUNTS

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. At all other times these accounts must be disabled. (PCI Requirement 8.5.6)

Requirement 9: Restrict Physical Access to Cardholder Data

PHYSICALLY SECURE ALL ACCESS TO CARDHOLDER DATA

At this time VSCC does not store any hard copy materials. At any point, if the need arises for VSCC to maintain hard copy material then the following will apply.

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

1. Printed reports containing cardholder data are to be physically retained, stored or archived only within secure office environments, and only for the minimum time deemed necessary for their use. (PCI requirement 9.6)
2. All hardcopy media containing cardholder data must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin). (PCI requirement 9.6)
3. Hardcopy material containing cardholder data should never be stored in unlocked or insecure containers or open workspaces. (PCI requirement 9.6)

4. All hardcopy material containing cardholder data must be easily distinguishable through labeling or other methods. (PCI requirement 9.7.1)
5. All confidential or sensitive hardcopy material must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked. (PCI requirement 9.7.2)
6. At no time is printed material containing cardholder data to be removed from any VSCC office without prior authorization from management. (PCI requirement 9.8)
7. Custodians of hardcopy media containing cardholder data must perform an inventory of the media at least annually. Results of inventories shall be recorded in an inventory log and maintained in the Business Office. (PCI requirement 9.9)

DESTRUCTION OF CARDHOLDER DATA

VSCC does accept payment via the phone. When VSCC does accept a phone payment the following will apply.

- All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)
- Hardcopy media must be destroyed by crosscut shredding, incineration or pulping so that cardholder data cannot be reconstructed. VSCC currently contracts with Shred-It to meet this requirement.(PCI requirement 9.10.1)

Requirement 10: Intentionally Omitted – Not Applicable to Current Operations

Requirement 11: Regularly Test Security Systems and Processes

TESTING FOR UNAUTHORIZED ACCESS POINTS

At least quarterly, VSCC will perform testing to ensure there are no unauthorized wireless access points present in the cardholder environment. (PCI Requirement 11.1)

VULNERABILITY SCANNING

At least quarterly, and after any significant changes in the network, VSCC will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Vulnerability scanning shall consist of external and internal scans. External scans must be performed on any public-facing devices, and conducted by an Approved Scan Vendor qualified by the PCI Security Standards Council. *Trustkeeper* software is used to perform these scans. Scan conducted after network changes may be performed by internal staff. Internal scans must be performed on all in-scope systems using an internally-approved scanning product. (PCI Requirement 11.2)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

INFORMATION SECURITY POLICY

VSCC maintains an Identify Theft Prevention/Red Flag policy that is reviewed annually. This policy addresses how the institution protects cardholder data, as well as other sensitive information. This policy must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1, 12.1.3)

Employees shall not use or otherwise employ employee-facing technologies to store, process or otherwise handle cardholder data. Employee-facing technologies include remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

The policies and procedures delineated in this document will apply to all employees and contractors involved in the processing, or other handling of cardholder data. (PCI requirement 12.4)

INCIDENT RESPONSE PLAN

The Director of Accounting and the Director of Information Technology will serve as Co-Directors of Incident Response. Designated members of VSCC's Information *Protection Committee* will serve on the *Incident Response Team* (IRT) in addition to personnel from Campus Security and Public Relations. The IRT shall establish, document, and distribute an *Incident Response Plan* to ensure timely and effective handling of all incidents. (PCI requirement 12.5.3)

1. Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents or red flags that an employee might recognize in their day to day activities include, but are not limited to:

A. Theft, damage, or unauthorized access (e. g. papers missing from their desk, broken locks, missing file logs, alert from campus police, or other evidence of a break-in or unauthorized physical entry).

B. Fraud – Inaccurate information identified within systems, logs, files or paper records.

2. Reporting an Incident

The Director of Accounting or the Director of Information Technology must be notified immediately of any suspected or real security incidents involving cardholder data. Unless it is reasonably certain that confidential information has not been compromised, the IRT must be assembled to assess the situation.

A. Employees should only communicate with their immediate supervisor or members of the Incident Response Team regarding any details or generalities

surrounding a suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Director of Public Relations.

B. Employees should document the date, time and the nature of the incident. Any additional information available will aid in the IRT responding in an appropriate manner.

3. Incident Response

The IRT will gather all information and take care to preserve the evidence. After reviewing information and evidence, the IRT will make an assessment as to whether or not confidential information was compromised. If a data compromise has occurred, the IRT must take whatever action is necessary to contain the damage and implement the following responses:

A. The IRT will notify the following:

1. Visa
2. MasterCard
3. Discover Card
4. Merchant Services
5. Local TBI/FBI Office who will determine additional notifications
6. U.S. Secret Service (if Visa payment data is compromised)
7. TBR Office of General Counsel

B. In concert with TBR legal counsel, the IRT will perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm

C. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Director of Accounting or the Director of Information Technology will work with legal and management to identify appropriate forensic specialists.

D. Eliminate the intruder's means of access and any additional vulnerability.

E. Research potential risks related to or damage caused by intrusion method used.

4. Root Cause Analysis and Lessons Learned

A. Not more than one week following the incident, members of the *Information Protection Committee* and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*.

B. Review other security controls to determine their appropriateness for the current risks.

C. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

SECURITY AWARENESS

VSCC shall implement and maintain a security awareness program with the intent of ensuring all employees who process, store, or are otherwise involved in handling cardholder data are aware of the importance of cardholder data security. (PCI requirement 12.6)

VSCC will ensure employees who have access to credit card data will receive security awareness training upon hire and at least annually. The security awareness program must provide multiple methods of educating employees, including posters, letters, memos, web-based training, meetings, or promotions. (PCI requirement 12.6.1)

THIRD PARTY SERVICE PROVIDERS

VSCC has verified the PCI compliance of the Point of Sale Terminals (Ingenico) used in collecting cardholder information as published by the PCI Security Standards Council (www.pcisecuritystandards.org). VSCC has also verified the use of *Trustkeeper* as an approved scanning vendor to perform required periodic scans, as published by the PCI Security Standards Council (www.pcisecuritystandards.org). Third party Hosts (Touchnet Information Systems, Inc. and XAP) will be required to provide certification of their PCI compliance annually.

IRT will implement policies and procedures to manage service providers. (PCI requirement 12.8) This process must include the following:

1. Maintain a list of service providers (PCI requirement 12.8.1)
2. Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2)
3. Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3)
4. Monitor service providers' PCI DSS compliance status (PCI requirement 12.8.4)

VSCC PROCUREMENT CARD POLICY

The College has a separate policy that governs the usage of procurement cards purchases. That policy is IV:02:02.

VSCC Sources: President's Cabinet, November 29, 2010