SUNY SCHENECTADY COUNTY COMMUNITY COLLEGE

## Financial

*Board of Trustees Policy*

| SUBJECT: | NUMBER: |
|---|---|
| Payment Card Industry Data Security Standard Policy | **6.7** |
| | **DATE:** **July 20, 2015** **Resolution #15-75** |
| | **SUPERSEDES:** |

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

# Payment Card Industry Data Security Standard Policy for SUNY Schenectady

## Policy Statement

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures listed in the Related Documents section of this Policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

## Applicability and Availability

This policy applies to all College offices that accept credit cards, the College's Information Technology Department and vendors that provide credit card processing services to the College. The most current version of this policy will be available on the SCCC web site.

## Adherence to Standards

Configuration standards must be maintained for applications, network components, critical servers, and wireless access points. These standards must be consistent with industry-accepted hardening standards as defined, for example, by SysAdmin Assessment Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

Configuration standards must include:

- updating of anti-virus software and definitions
- provision for installation of all relevant new security patches within one month
- prohibition of group and shared passwords

## Handling of Cardholder Data

Distribution, maintenance, and storage of media containing cardholder data must be controlled. Procedures must include periodic media inventories in order to validate the effectiveness of these controls.

Procedures for data retention and disposal must be maintained by each department accepting credit cards for payment and their credit card processing vendors and must include the following:

- legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data

- provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data
- coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to
- a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, an audit process, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements
- destruction of media when it is no longer needed for business or legal reasons as follows:
- cross-cut shred, incinerate, or pulp hardcopy materials
- purge, degauss, shred, or otherwise destroy electronic media such that data cannot be reconstructed

Credit card numbers must be masked when displaying cardholder data. Those with a need to see full credit card numbers must request an exception to this policy using the exception process.

Unencrypted Primary Account Numbers may not be sent via email.

**Access to Cardholder Data**

**Procedures for data control must be maintained and must incorporate the following:**

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
- Assignment of privileges is based on individual persom1el's job classification and function
- Requirement for an authorization form signed by management that specifies required privileges
- Implementation of an automated access control system

Approved by the SUNY Schenectady Board of Trustees, July 20, 2015, Resolution # 15-75