NORTH HENNEPIN COMMUNITY COLLEGE

Number: 5.23.1.10	**Name:** Payment Card Industry (PCI) – Technical Requirements
Author: Kristine Boike	**Custodian:** CIO
Effective Date: August 27, 2012	**Next Review Date:** AY2015-2016
Regulatory Authority: • MnSCU Board Policy 5.22, **Acceptable Use of Computers and Information Technology Resources** • MnSCU Guideline 5.23.1.10, **Payment Card Industry – Technical Requirements** • MN Statue 43.A38, **Code of Ethics for Employees in the Executive Branch**	

Part 1. Purpose

This guideline emphasizes many of the minimum requirements necessary to comply with the Payment Card Industry Data Security Standards (PCI DSS). While PCI DSS is not an actual law, it is a standard enforced by the credit card industry, and the banks have stated and upheld the policy that they will no longer accept business from non-PCI compliant merchants. Please see MnSCU 5.23.1.10 for the entire MnSCU Requirement.

Part 2. Applicability

Subpart A.

These standards are designed to protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with North Hennepin Community College. This policy is intended to be used in conjunction with the complete **PCI-DSS requirements** as established and revised by the PCI Security Standards Council.

PCI DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The twelve (12) requirements apply to all organizations that store, process or transmit cardholder data.

Subpart B. Requirements

The twelve (12) requirements are:

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor supplied defaults for system passwords and other security parameters.
3. Protect cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update anti-virus software and programs.
6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Subpart C. Common Practices

Common Practices: These are some common practices that help to protect cardholder information:

1. Do not distribute credit card information in any unencrypted format.
2. Do not access files to which you have not been granted explicit permission to by the owner.
3. Ensure that you have appropriate training on the applications which you use.
4. If you find an error or unsecured cardholder data, notify a manager or the helpdesk.
5. Protect you own information as well as others.

What is cardholder data:

		Data Element	**Storage Permitted**	**Render Stored Account Data Unreadable per Requirement 3.4**
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data	Full Magnetic Stripe Data	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

Subpart D. Application
All NHCC departments that collect, maintain or have access to credit card information must comply with PCI policy. These currently include:

1. Adult Education and Training
2. Accounting and Fees
3. Foundation
4. NHCC Bookstore

Review Action	Date(s)
Campus Community Review Period	March 21, 2012 – April 4, 2012
Shared Governance Council Review	April 27, 2012
Labor/Management Meetings Review	MAPE April 5, 2012 MMA April 5, 2012 AFSCME April 26, 2012
Student Senate Review	April 26, 2012
President Approval	June 4, 2012
Campus Community Dissemination	July 2012

History

- New requirements – adopted August 27, 2012