Durham College Policy and Procedure

TYPE:	Administrative
TITLE:	Payment Card Industry Sustainability
NO.:	ADMIN-277
RESPONSIBILITY:	Chief Financial Officer and Vice-President, Administration and Associate Vice-President, Information Technology
APPROVED BY:	Durham College Leadership Team
EFFECTIVE DATE:	November 2022
REVISED DATE(S):	
REVIEW DATE:	November 2025

1. Introduction

The Payment Card Industry (PCI) established the Data Security Standard (DSS) that all merchants must adhere to in order to accept payments by credit card. The DSS is a set of information security best practices designed to keep credit card information safe at rest and in transit.

Durham College maintains a dedicated PCI Cardholder Data Environment (CDE) for all payment processing functions that are needed on or off campus. This environment has various maintenance activities that must be performed to both maintain compliance with the PCI standard, and maintain the integrity of the environment. The tasks required are a combination of operational and technical procedures.

All merchants using payment processing technologies deployed on Durham College networks, whether employees, students, vendors, contractors or business partners, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Vice-President, Administration and Chief Financial Officer (CFO) or the Associate Vice-President (AVP), Information Technology.

2. Purpose

This policy and procedure establishes the activities required for the College to maintain compliance of the PCI standard, and maintain the integrity of the PCI CDE.

3. Definitions

Refer to Durham College's Standard Definitions.

4. Policy statements

4.1. Finance shall ensure that the following activities are performed.

4.1.1. Ensure that payments taken over the phone leverage the PCI acceptable outsourced solution. Finance will ensure that there is an adequate process in place for taking card payments over the phone, and users are aware that the process needs to be followed.

4.1.2. Regularly, and prior to the annual assessment, update inventory of Critical PCI-Related Technology such as cash registers and PIN pads.

4.1.3. Maintain a list of vendors or service providers where their products are used to process credit card payments on behalf of the College. Ensure the service providers' PCI DSS compliance is monitored regularly, and prior to the annual assessment.

4.1.4. Maintain a written agreement that includes an acknowledgement that the relevant service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s cardholder data or sensitive authentication data, or manages the customer's CDE on behalf of a customer.

4.1.5. Ensure there is an established process for engaging PCI-related service providers including proper due diligence prior to engagement.

4.1.6. Ensure new vendors wanting to accept credit card information on campus are not allowed to process electronic transactions using the campus network infrastructure. New vendors should use cellular enabled PIN pads for in person transactions wherever possible. Exceptions need approval from the Director, ICT Infrastructure.

4.2. Managers responsible for PCI account access and management shall ensure the following activities are performed as needed:

4.2.1. Creating, controlling and managing user accounts that can access the CDE.

4.2.2. Every user must use a unique user ID and a personal secret Password for access to campus information systems and networks.

4.2.3. User accounts must be created with the lowest required access level appropriate for the user, following the Role-Based Access Control principle.

4.2.4. User privileges are to be reviewed on a regular basis and removed if the privileges are no longer required.

4.2.5. Mechanisms such as tokens, digital certificates, or other means of multiple Authentication Factors may be used in addition to Passwords for the identification and authentication of users, and must also be unique to each user.

4.2.6. Where possible, users must be forced to change their Password when they first log on to the system.

4.3. Account management

4.3.1. User accounts are only to remain active for the period required for users to fulfill their responsibilities.

4.3.2. Central IT accounts of staff will be disabled once an employee is no longer working at Durham College.

4.4. Password Aging Rule

Administrators who operate their own systems associated with the CDE are responsible for implementing a process to force aging of Passwords at least every 90 days.

4.5. Departments or schools processing credit cards shall ensure that the following activities are performed on a regular basis:

4.5.1. Ensure that they understand the PCI standards by signing an acknowledgment declaration.

4.5.2. Inspect PIN pad devices for signs of tampering or substitution such as broken seals or incorrect serial numbers.

4.5.3. Ensure that credit card information at rest is encrypted if electronic, and physically secured if on paper.

4.5.4. Ensure that dual factor authentication is used to access payment workstations remotely.

4.5.5. Ensure that relevant information security awareness training is completed annually.

4.6. IT Services shall ensure that the following activities are performed on a regular basis.

4.6.1. Ensure that the network and data flow diagram(s) accurately reflect the network architecture.

4.6.2. Ensure that the credit card data information in transit is secure and encrypted within the campus infrastructure.

4.6.3. Review firewall and router rulesets pertaining to the PCI zone at least every six months.

4.6.4. Regularly, and prior to the annual assessment, update inventory of all CDE locations, hardware / software / applications and networks.

4.6.5. Update configuration standards as necessary, images for all system components. Ensure the workstations used are hardened and comply with the PCI standard.

4.6.6. Review vulnerabilities in a timely fashion once the software publisher provides security alerts.

4.6.7. Install applicable vendor-supplied patches: critical within one month, non-critical within three months for all IT Assets in the CDE.

4.6.8. Scan for the presence of all unauthorized network equipment in the PCI zone.

4.6.9. Ensure that dual factor authentication is used to administer or access payment workstations remotely.

4.6.10. All remote-access technologies must be configured to automatically disconnect sessions after 30 minutes of inactivity.

4.6.11. All remote-access technologies and associated accounts used by vendors and business partners to access the CDE must be activated only when needed, with immediate deactivation after use. Activating these remote-access paths and accounts requires submitting a request to the IT Service Desk.

4.7. If cardholder data is available through remote-access technologies, special precautions must be taken.

4.7.1. Copying, moving, or storing cardholder data onto local hard drives and removable electronic media is prohibited.

4.7.2. Personnel with a valid business need to see cardholder data must be authorized by the Director, Information Security, and the data must be protected accordingly.

4.8. Review, and update as necessary, the organization’s information security related policies, procedures, and standards from a PCI perspective.

4.9. The Director, Information Security shall ensure that the following activities are performed on a regular basis:

4.9.1. Confirm the location(s) of the CDE and flow of cardholder data and ensure that they are included in the PCI DSS scope, including backups.

4.9.2. Review Compensating Controls to ensure that they are properly documented and are still applicable.

4.9.3. Engage and manage an Approved Scanning Vendor (ASV) to conduct external vulnerability scanning.

4.9.4. Conduct a formal threat risk assessment at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.).

4.9.5. Run an awareness program for employees processing credit cards. Confirm they've read and understand the policy/procedures.

5. Procedure

The PCI account management and access procedures are as follows:

5.1. Authentication

All users are required to follow strict Password management procedures. In some cases, these requirements will be implemented by the owners of the relevant systems. In others, it will be the responsibility of the user to ensure these procedures are followed. The procedures below are the bare minimum requirement. If a system has procedures which are more restrictive than those outlined below, continue with the more restrictive procedures.

5.2. Initial Passwords or Password Resets

5.2.1. Passwords for new user accounts or after a Password reset must be set to a unique random value.

5.2.2. The unique random value Password must be changed on first use. If possible, this will be required by the system. If the user is not prompted by the system to modify the Password, it is their responsibility to change the Password.

5.2.3. Users must follow best practices for secure Passwords. Examples can be found at http://servicedesk.durhamcollege.ca.

5.3. Password Aging Rule

System owners and administrators are responsible for ensuring users regularly

change their Passwords. Enforce a Password change at least every 90 days. Limit Password reuse to the last 6 Passwords.

5.4. Multi-Factor Authentication

In addition to Passwords, there will be situations where multiple Authentication Factors are required.

The following scenarios require multi-factor authentication:

- An administrator is accessing the CDE from anywhere other than the server console.
- A user is accessing the CDE through a Virtual Private Network (VPN).
- Users are required to contact IT Services to obtain multi-factor authentication access if either of these situations apply to them.

5.5. Re-Authentication

5.5.1. Any time a user steps away from a workstation that has access to the CDE, the user should lock their computer to prevent inadvertent access by another user. At a minimum, screensavers that lock the computer should start after at most 15 minutes of inactivity, requiring re-authentication to access the system.

5.5.2. Systems should also have session time-outs, which require a user to re-authenticate.

5.6. PCI Account Access and Management

Managers responsible for access to payment processing technology in department specific software are responsible for regularly reviewing accounts. For example, the manager of the bookstore would need to review the bookstore staff accounts to ensure staff have the appropriate access. Generate a quarterly report, or capture the user management page as a screenshot, as required that contains the following types of accounts, and remediate as necessary:

- Locked accounts
- Disabled accounts

5.7. Revoking Access

5.7.1. Access must be revoked for terminated users immediately.

5.7.2. User credentials and other authentication methods need to be revoked as soon as possible upon an employee's departure.

5.7.3. Upon quarterly review of accounts, inactive accounts must be deactivated (at least every 90 days).

5.7.4. Accounts must be locked out after 6 unsuccessful authentication attempts.

5.8. Monitoring Inappropriate Account Usage

System owners and administrators are responsible for ensuring that old accounts are not being used. Monitor account usage to identify dormant accounts, and determine appropriate action for those accounts. Monitor any attempts to use deactivated accounts.

6. Roles and responsibilities

6.1. The CFO is responsible for ensuring that the appropriate policies and procedures are in place to handle credit card data securely and that the Critical PCI-Related Technology inventory is updated.

6.2. Financial Operations is responsible for keeping a PCI-related list of vendors.

6.3. Financial Operations and IT Services are responsible to ensure that new vendors are not permitted to use the campus network to process payment transactions.

6.4. The AVP, IT is responsible for ensuring policies regarding PCI sustainability are carried out; confirming that diagrams, technology inventories, vulnerability list, and policy maintenance is done regularly as dictated by PCI DSS.

6.5. The Director, Information Security is responsible for reviewing, monitoring, and updating compensation controls, security policy, conducting formal risk assessments, running awareness and training programs, and ensuring service provider compliance.

6.6. The Director, ICT is responsible for approval, deployment, and use of critical devices, multi-factor authentication implementation, and arranging for the documentation of critical device inventory, configuration of critical devices, and remote access technologies and reviewing firewall and router rule sets.

6.7. System administrators are responsible for running and maintaining anti-virus software and scans, deactivating user accounts (including third-party accounts) as dictated by PCI, internal and external security/vulnerability scans, testing for unauthorized access and access points, and updating CDE location and flow diagrams.

7. Accessibility for Ontarians with Disabilities Act considerations

Accessibility for Ontarians with Disabilities Act (AODA) standards have been considered in the development of this policy and procedure and it adheres to the principles outlined in the College's commitment to accessibility as demonstrated by the Multi-Year Accessibility Plan.

8. Non-compliance implications

Failure to comply with this policy could result in loss of access to Durham College information technology services and equipment, disciplinary action up to and including suspension or termination of an employee, and/or legal action that could result in criminal or civil proceedings.

9. Related forms, legislation or external resources

- Payment Card Industry Data Security Standards, authored by the PCI Security Standards Council: https://www.pcisecuritystandards.org/