AD16	Payment Card Industry Data Security Standards
Classification:	Administration
Responsible Authority:	Chief Digital Officer
Executive Sponsor:	Vice President, Finance and Administration
Approval Authority:	Algonquin College Executive Team
Date First Approved:	2013-07-02
Date Last Reviewed:	2024-03-25
Date to Complete Mandatory Review:	2026-03-25

PURPOSE

This policy sets forth the guidelines required by the College regarding Payment Card Industry Data Security Standards (PCI DSS) for processes and technology involved in acceptance, processing, and transmission of debit and credit cardholder account data.

SCOPE

This policy applies to all Algonquin College business units, departments, schools and their employees (which includes faculty, staff and students) involved in accepting, processing, or transmitting cardholder account data for payments on behalf of Algonquin College. This includes all payment transactions involving credit cards, debit cards, or pre-paid cards branded with one of the five payment card brands that are part of the PCI Security Standards Council (Visa, MasterCard, American Express, JCB International and Discover Financial).

DEFINITIONS

Word/Term	Definition
Acquirer	Also referred to as “merchant bank,” “acquiring bank” or “acquiring financial institution.” An entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Algonquin College Merchant	A business unit, department, school and their employees (which includes faculty, staff, students and volunteers) authorized by Algonquin College to process payment card transactions on behalf of the College.
Card Verification Code or Value	The rightmost three or four-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the primary account number (PAN) on the face of all payment cards. Depending on the card issuer, this information is called CID, CVC2, CVV2 or CAV2.
Cardholder Account Data	Consists of cardholder data and sensitive authentication data.
Cardholder Data	At a minimum, cardholder data consists of the full payment card Primary Account Number (PAN). Cardholder data may also exist in the

	form of the full PAN, plus any of the following: cardholder name, expiration date and/or service code.
Cardholder Data Environment	The people, processes and technology involved in acceptance, processing or transmission of cardholder account data, including any connected system components.
Merchant	An entity that accepts payment cards bearing the logos of any of the five members of the PCI SSC as payment for goods and/or services.
Merchant Account	A bank account that enables the holder to accept payment cards bearing the logos of any of the five members of the PCI SSC.
Merchant Account Owner	The manager responsible for an Algonquin College business process that involves the acceptance of payment cards into a Merchant Account.
Network Segmentation	Also referred to as “segmentation” or “isolation”, network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the Cardholder Data Environment and thus reduces the scope of the PCI DSS assessment.
Payment Application Data Security Standard	The Payment Application Data Security Standard covers secure payment applications to support PCI DSS compliance.
Payment Brands	The founding members of PCI SSC, which are Visa, MasterCard, American Express, JCB International, and Discover Financial.
Payment Card	Credit card, debit card or pre-paid card branded with the logo of any of the payment brands.
Payment Card Industry Data Security Standard	The Payment Card Industry Data Security Standard was developed to enhance cardholder data security and facilitate consistent data security measures by providing a baseline of technical and operational requirements designed to protect cardholder data.
Payment Card Industry Security Standards Council	The Payment Card Industry Security Standards Council is an independent body providing oversight of the development and management of PCI DSS. The founding members of PCI SSC are Visa, MasterCard, American Express, JCB International, and Discover Financial.
Payment Card Privilege	Refers to the privilege which merchants have to accept payment cards for payment transactions.
Qualified Integrator and Reseller	A Qualified Integrator and Reseller is an organization that is authorized by the PCI Security Standards Council to implement, configure and/or support PA-DSS payment applications. The PCI Council lists all qualified QIRs on its website.
Self-Assessment Questionnaire	A Self-Assessment Questionnaire is an assessment document that is used by a merchant to validate its own compliance with the PCI DSS. Algonquin College utilizes several different SAQs covering its various merchant account areas.
Sensitive Authentication Data	Sensitive Authentication Data represents security-related information (including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

System Component	Any network component, server, or application included in or connected to the Cardholder Data Environment.

POLICY

1. PCI DSS Compliance Requirements:

   As a merchant that collects, processes and transmits cardholder data, Algonquin College is required to be PCI DSS compliant by the PCI Security Standards Council (PCI SSC). Non-compliance exposes the College to significant risks including but not limited to:

   - Payment card compromise, theft and financial fraud;
   - Cardholder identity theft;
   - Incident response and security breach recovery costs;
   - Fines and penalties for compromise, including increased cost per processed transaction;
   - Termination of payment card privileges;
   - Prevention from entering into new lines of business;
   - Loss of customer trust and business;
   - Damage to reputation and brand; and
   - Legal liabilities.

2. Algonquin College Merchant Accounts:

   Any business unit, department or school establishing a new operation to process payment card transactions must submit a business case to the College Treasury Department. They will review and approve submitted business cases for all prospective Merchant Account Owners.

   Upon approval from the College Treasury Department, the business unit must submit a formal project request to its ITS Business Relationship Manager and the Associate Director, Information Security and Privacy for an IT business analysis, security review and implementation project. This step may be performed as a part of a larger College Business Plan/Operating Initiative process.

   Any business unit, department or school establishing a new operation to process payment card transactions must formally request and receive an approved Algonquin College merchant account and merchant identification number (MID) from the Algonquin College Treasury Department prior to processing any payments.

   Any Merchant Account Owner or Merchant Location implementing more than one payment transaction process within the business unit, department or school must formally request and receive an approved merchant identification number (MID) from the Treasury Department for each payment process, prior to processing any payments.

3. Algonquin College Treasury Department:

The Algonquin College Treasury Department is the only administrative body authorized to create/open merchant accounts. All merchant accounts must be approved in writing by the Treasury Department. All merchant accounts must have an associated Merchant Account Owner.

The Algonquin College Treasury Department is the only administrative body that is authorized to apply for, and facilitate the processing of a merchant identification number (MID) with our Acquirer.

4. Opening Bank Accounts:

   All Algonquin College business units, departments and schools are prohibited from opening a bank account or any type of account (e.g. PayPal) to receive payments in the name of the College.

   The Algonquin College Treasury Department is the only business unit authorized to establish bank accounts to receive payments on behalf of the College. This includes all bank accounts bearing a College campus address.

   All bank accounts opened on behalf of an Algonquin College Merchant Location or business unit must include signatures from two authorized bank signing officers.

5. Chief Financial Officer, Finance and Administrative Services:

   Provides management oversight for all Finance related decisions and directions with respect to payment cards and reconciliations.

6. Treasury Supervisor, Finance:

   Provides day-to-day management of Algonquin College merchant accounts, including the review and approval of requests for new accounts or changes to existing accounts, and liaising with the College's acquirer.

7. Chief Digital Officer (CDO), Information Technology Services (ITS):

   Provides management oversight for all IT related decisions and directions with respect to the card data environment.

8. Associate Director, Information Security and Privacy (ITS):

   Provides oversight and governance for all Algonquin College PCI DSS compliance related matters, including the authority to review and audit all payment related systems. All initiatives and projects to be carried out on behalf of Algonquin College which involve payment card processing must be reviewed and approved by the Associate Director prior to implementation, and must comply with requirements specified by the College and the PCI DSS compliance standards. The Associate Director is responsible for formal PCI DSS communications within the College, including the maintenance of a PCI DSS stakeholder advisory committee. The Associate Director may delegate his/her responsibilities as appropriate.

9. Merchant Account Owners:

   Algonquin College Merchant Account Owners are staff, officially appointed by the Treasury Department, responsible for an Algonquin College business process that involves the acceptance of payment cards. They are responsible for ensuring the people, processes and technologies involved in accepting, processing or transmitting cardholder data within their area, including connected or supporting systems, comply with the PCI DSS and related Algonquin College policies, standards and procedures.

10. Electronic Storage and Transmission of Cardholder Account Data:

    Cardholder account data must not be stored electronically anywhere within the Algonquin College IT environment (e.g. computer systems, network drive, database server) nor transmitted/received by electronic messaging (e.g. email, instant messaging).

    Email, instant messaging and text messaging are not acceptable methods of sending or receiving payment card account information. Emails, instant messages and text messages received containing card holder data must be permanently deleted immediately.

11. Paper Retention and Disposal:

    Paper records of financial transactions that contain cardholder data must be securely stored at all times. Records are to be retained for a limited period consistent with the needs of the business. Storage and retention period must be approved by the Associate Director, Information Security and Privacy.

12. Third Parties Contractual Agreements:

    Due diligence must be followed when engaging external third parties to provide solutions and services related to the College's PCI DSS program.

    All external parties including but not limited to service providers, qualified integrators and resellers (QIR), program assessors, and acquirers, must be contracted using a written agreement that details their involvement, activities and responsibilities related to the College's PCI DSS program. Responsibilities must be captured in a Responsibility Matrix document. The agreement, and responsibility matrix must be approved by the Associate Director, Information Security and Privacy. Both documents must detail the protection mechanisms afforded to any cardholder data held in their possession.

13. Incident Response:

    In the event of a security incident related to Algonquin College payment processes or systems in scope for PCI DSS compliance, such as a security breach of cardholder data, the Associate Director of Information Security and Privacy must be notified immediately, and is responsible for leading the execution of the PCI DSS Security Incident Response Plan.

14. Change Management:

    Any change to Algonquin College business processes, systems, infrastructure or applications that have or might have a PCI DSS compliance implication, or that impacts processing of credit card payments, must be reviewed and approved by the Associate Director, Information Security and Privacy prior to implementation.

    Any minor or major changes, or maintenance activities to College systems, infrastructure or applications that may impact the PCI DSS environment, PCI DSS compliance or the processing of debit and credit card payments must be formally documented in a change log. All changes must be detailed as well as adequately maintained and archived. This applies to changes made by employees, vendors, and third-parties.

15. Accounts and Privileges:

    User accounts with access to systems in scope for PCI DSS compliance must be restricted to least privileges necessary to perform job responsibilities. Privileged accounts for individuals must be assigned based on job function, and must be authorized by the Merchant Account Owner or delegate.

    Accounts and privileges assigned to individuals who are no longer employees, or who no longer have payment process related responsibilities, must be terminated immediately.

16. System Configuration and Operations:

    For all systems in-scope for PCI DSS compliance, Algonquin College system configuration standards and operational security procedures must be followed for configuring and operating network and firewall components, application components, servers and all other system components.

17. Technology Use:

    No technology systems shall be used within the security controlled Cardholder Data Environment, nor shall any user access to technology systems be authorized unless:

    - Explicit approval by the Associate Director, Information Security and Privacy is obtained, prior to implementation.
    - A list of all such technology systems is provided to the Associate Director, Information Security and Privacy, and the list maintained thereafter.
    - Specific acceptable network locations for and usage of technology systems is defined and approved.
    - All technology systems are appropriately labeled with information that references system owner, contact information and purpose.
    - Strong, multi-factor authentication is used for remote access to the Cardholder Data Environment. Remote Access is any access that originates from outside the Algonquin network, such as employees working from home or vendors providing support from remote locations.
    - Remote access technologies used by external party vendors and solution providers are only activated for specific periods when needed, and automatically

disconnect after that time as well as when there is a specific period of inactivity. These periods shall not exceed eight hours.
- Payment applications are PA-DSS approved and validated as per the following:https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications

18. Security Awareness and Training Program:

    Employees with work functions that include accepting, transmitting and/or processing payment card information must, upon being hired, read this Algonquin College PCI DSS policy AD16 and undergo an initial mandatory security awareness and training program. These employees must subsequently undergo mandatory PCI DSS awareness and training program on an annual basis. Each Merchant Account Owner is responsible for ensuring that their required team members complete the training.

19. Policy Review:

    The Algonquin PCI DSS policy and procedures must be reviewed every two years, or earlier if there is substantive change within the PCI DSS environment, and updated as required to reflect changes to PCI DSS standards, other regulations, policies, business objectives or changes to the Cardholder Data Environment.

20. Policy Compliance:

    All Algonquin College people, process and technology that support business processes involving payment cards must comply with this policy. Failure by Algonquin College Merchant Account Owners to comply with this policy to the satisfaction of the Associate Director, Information Security and Privacy may result in the revocation of the Merchant Account Owner's payment card privileges.

PROCEDURE

	Action	Responsibility
1.	**PCI DSS Compliance Oversight and Governance**	
1.1	Achieve and maintain Algonquin College PCI DSS annual compliance certification.	Associate Director, Information Security and Privacy, affected ITS Managers, Merchant Account Owners
1.2	Utilize and document appropriate PCI DSS Self-Assessment Questionnaire(s) (SAQs) annually on behalf of the entire College.	Associate Director, Information Security and Privacy
1.3	Review annual PCI DSS SAQs and provide attestation to their accuracy and completeness.	Vice-President, Finance and Administration
1.4	Provide appropriate interpretation and communication of PCI DSS compliance guidelines and best practices.	Associate Director, Information Security and Privacy
1.5	Ensure that Algonquin College contractual agreements, where applicable, stipulate adherence to PCI DSS requirements.	Merchant Account Owners

1.6	Implement a formal PCI DSS awareness and training program to educate employees on the importance of PCI DSS compliance.	Associate Director, Information Security and Privacy
2.	**Management of Algonquin College Merchant Accounts**	
2.1	Make requests for new merchant account identification number and/or Point of Sale (POS) devices in writing to the Treasury Department	Merchant Account Owners
2.2	Provide business case (if required) for new merchant number or Point of Sale device.	Merchant Account Owners
2.3	Provide sufficient details of intended business processes to the Associate Director, Information Security and Privacy to determine the relevant sections of the appropriate PCI DSS SAQ to be completed.	Merchant Account Owners
2.4	Review and approve submitted business cases for all prospective Merchant Account Owners.	Treasury Department
2.5	Provide written approval and instruction to the new Algonquin College Merchant Account Owner.	Treasury Department
2.6	Implement an appropriate payment solution for an approved Algonquin College merchant after approval by Associate Director, Information Security and Privacy, and Treasury Department.	Information Technology Services
2.7	Respond to relevant sections of the appropriate PCI DSS SAQ and submit information and evidence to the Associate Director, Information Security and Privacy for review.	Merchant Account Owners
2.8	Review and validate Algonquin College Merchant Account Owner responses to the appropriate PCI DSS SAQ.	Associate Director, Information Security and Privacy
2.9	Revoke Algonquin College merchant payment card privileges as deemed appropriate.	Treasury Department
3.	**Implementation, Controls, and Processes**	
3.1	Develop and maintain business process controls in compliance with PCI DSS requirements and as advised by the Associate Director, Information Security and Privacy.	Merchant Account Owners
3.2	Design, integrate and implement payment solutions for all Algonquin College Merchant Account Owners in compliance with PCI DSS requirements, including the development or the purchase of appropriate software or services to be used by Algonquin College Merchant Account Owners.	Merchant Account Owners, Information Technology Services, Manager, Information Security and Privacy
3.3	Maintain, support and monitor Algonquin College payment system components in compliance with PCI DSS requirements.	Merchant Account Holders, Information Technology Services
3.4	Restrict access to records on a business need-to-know basis. Securely store paper records of cardholder data only for a specific limited retention period and only if there is a business justification. At	Merchant Account Owners

	the end of the retention period, ensure that records are crosscut shredded, incinerated or otherwise securely destroyed to ensure that records cannot be reconstructed.	
3.5	Maintain an up-to-date list of devices that capture payment card data via direct physical interaction. The list must include - at a minimum - the make, model, serial number, owner and location of each device.	Merchant Account Owners

RELATED POLICIES

AD02: Freedom of Information and Protection of Privacy
IT01: Information Security

RELATED MATERIALS

PCI DSS Compliance - Payment Terminal Security Procedures

PCI DSS Standards and Supporting Documents:
https://www.pcisecuritystandards.org/document_library