Lakehead University | University Secretariat

Lakehead University Payment Card Industry (PCI) Standards Policy

Category: Financial;
Jurisdiction: Vice President, Administration & Finance;
Approval Authority: Executive Team;
Established on: July 1, 2017;
Amendments: None.

Who Should Read this Policy: All persons who have access to credit card information, including:

- Every employee that accesses handles or maintains credit card information. Lakehead University employees include full-time, part-time, and hourly staff members as well as student workers who access, handle or maintain records.
- Employees who contract with service providers (third party vendors) who process credit card payments on behalf of Lakehead University.
- Employees who manage events and require payment-processing capabilities (e.g. Online, Portable Point of Sale device).

Name: PCI DSS stands for Payment Card Industry Data Security Standard (PCI DSS), and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

1. **Purpose:** The Payment Card Industry Data Security Standards (PCI DSS), are a set of comprehensive requirements for enhancing payment account data security, was

developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

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 threat s. The standards apply to all organizations that store, process or transmit cardholder data.

2. **Reason for the Policy**: The 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 the University. 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.

3. **Entities Affected by this Policy**

   All departments that collect maintain or have access to credit card information. These currently include but are not limited to:

   - Accounts Receivable: accept and process credit cards for payment of student accounts and miscellaneous receivables; both in person and through online solutions.
   - University Bookstore: accept and process credit cards for sale of books and sundries both online and in person.
   - Admissions: accept deposits towards registration.
   - Recruitment (Domestic and International): Accept application fees.
   - External Relations: accept and process credit cards for donations and alumni events.

- Residence and Conference Services: accept and process credit cards for deposits and room rentals.
- Parking/Security: accept and process credit cards for payment of a parking permit and infractions.
- Enrolment Services: accept and process credit cards for payment of miscellaneous service charges such as Program Change Fee, Convocation Fee, Transcript Fee, and Invigilation Fee.
- Student Health and Counselling Services: accept credit cards for payment of health services.
- Faculty of Education/Professional Development in Education. Accept deposits towards registration.
- Athletics: accept credit cards for the payment of memberships and intramural sports.

All departments managing or sponsoring events that use online payment services approved by the Manager of Accounts Receivable to collect payments through an access point that has been deemed PCI compliant by the University , even though these entities do not have access to credit card information, including:

- All departments hosting/sponsoring student activities/programs with payments through online payment service approved by the Manager of Accounts Receivable, (e.g.: Student leadership, Pre-Orientation).
- All academic departments hosting/sponsoring academic conferences/programs with payments through online payment service approved by the Manager of Accounts Receivable.
- All departments who have relationships with third party vendors that serve as access points through which Moneris, or any other payment services approved by the Manager of Accounts Receivable, are reached. These departments must confirm PCI compliance on the part of the vendor when Lakehead University's merchant accounts are not used.

- Athletic: uses Thriva for camps registration.

4. **List of Third Party vendors that process and store credit card information for Lakehead University using University merchant accounts include, but are not limited to:**
   - Orbis: for MySuccess related transactions
   - Paypal: for MyInfo payment processing.
   - Cale Systems: Pay and Display parking meters.
   - Tomahawk Technologies: Parking tickets and parking pass sales.
   - Carleton Technologies: Bookware bookstore POS.
   - Innosoft Fusion: Athletics for seminars and memberships.

5. **Definitions**

- PCI DSS: Payment Card Industry Data Security Standard
- Merchant Account: A relationship set up by the Manager of Treasury and Ancillary Fund Accounting between the university and a bank in order to accept credit card transactions. The merchant account is tied to a general ledger account to distribute funds appropriately to the department (owner) for which the account was set up.
- Financial Data Manager (FDM): The Associate Vice-President Financial Services for the University who has oversight responsibility for this policy. The FDM will approve appointment of the Compliance Coordinator.
- PCI Compliance Coordinator: Financial Projects Manager, who, under the direction of the FDM, will be responsible for staying abreast of changes to PCI DSS requirements, suggesting updates to the policy, coordinating training, and serving as point of contact for the University community with regard to assessment surveys or other PCI issues.
- PCI Department Coordinators: Representatives within departments who are responsible for ensuring that all departmental personnel with access to credit card data receive appropriate training, read this policy, and sign off on having read this policy. The PCI department coordinator will also be responsible for completing the annual department

survey or assessment as required. Appointments of PCI Department Coordinators must be approved by the FDM.

- Credit Card Data: Full magnetic stripe or the PAN (Primary Account Number) plus any of the following:
- Cardholder name
- Expiration date
- Service Code
- PCI Security Standards Council: The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.
- Self-Assessment: The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.
- PAN: Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.
- Level of Compliance: Credit card companies and financial institutions validate that vendors are rated based on their volume of transactions. The rating that a company receives determines the process that they must go through in order to be validated. There are four levels of PCI Compliance, with level 1 being the most stringent and level 4 being the least stringent. If a merchant suffers an attack that has caused account data to be compromised, the merchant level requirement goes up to level 1 automatically. Based on the number of credit card transactions processed annually across the campus (fewer than 20K per year), and the fact that the University has not experienced a breach; Lakehead University would be classified as Level 4. Lakehead University must complete an annual self-assessment questionnaire (SAQ).
- PCI DSS Version 3.0 Requirements: University policy prohibits the storing of any credit card information in an electronic format on any computer, server or database (this includes Excel spreadsheets). It further prohibits the emailing of credit card information. The following list communicates the full scope of the compliance requirements but based on the University policy that prohibits storing of credit card information

electronically and Lakehead University's practice of utilizing third-party vendors for web based credit card processing, some listed requirements may not be relevant.

6. Compliance Goals

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and systems	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Protect stored card holder data Encrypt transmission of cardholder data across open, public networks
Support a Vulnerability Management Program	Make available anti-virus software and other supports to protect systems
Implement Strong Access Control Measures	Restrict access to cardholder data by business need to know Identify and authenticate to system components Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Regularly test central security systems and processes

7. **Procedure**: Lakehead University requires compliance with PCI standards. To achieve compliance, the following requirements must be met:

a. General Requirements

- Credit card merchant accounts must be approved by the Manager of Treasury and Ancillary Fund Accounting.

- Management and employees must be familiar with and adhere to the PCI-DSS requirements of the PCI Security Standards Council.
- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by Financial Services.
- An inventory of card readers and card processing terminals will be maintained and updated as needed, by the PCI Compliance Coordinator.
- New employees must undergo PCI training upon hiring.
- Existing employees must undergo PCI training annually.
- Access to the cardholder data environment must be restricted to only those employees with a need to access and physical controls must be in place to protect the cardholder data environment.
- Terminals/readers must be routinely examined for evidence of tampering and any evidence brought to the attention of the PCI Compliance Coordinator.
- Management using Paypal or other Financial Services approved online payment services for event payments must ensure that all personnel within their department understand that Lakehead University prohibits anyone from accepting credit card information or processing credit card payments on behalf of the “customer”.
- Employees managing/sponsoring events for which Paypal or other approved online payment services are used must confirm knowledge of and adherence to the above policy when requesting Paypal or other approved online payment service access/mailbox from Financial Services.
- Management in departments must confirm that the third party vendors through whom they are accessing Paypal or other approved online payment services are PCI compliant. Minimum compliance evidence, up to date self-assessment questionnaire (SAQ) for the vendor company.

b. Storage and Disposal

- Credit card information must not be entered/stored on any electronic device including University network servers, workstations, laptops, tablets and cell phones.

- Credit card information must not be transmitted via email.
- Web payments must be processed using a PCI-compliant service provider approved by Financial Services.
- Any paper documents containing credit card information should be limited to information required to transact business, those individuals who have a business need to have access, should be in a secure location, and must be destroyed via cross-cut shredding or placement in a secure shred bin once business needs no longer require retention.
- All credit card processing machines must be programmed to print-out only the last four or first six characters of a credit card number.
- Sensitive cardholder data must be destroyed when no longer needed for reconciliation, business or legal purposes. In no instance shall this exceed 45 days and should be limited whenever possible to only 3 business days. Secured destruction must be via cross-cut shredding in house or with a third-party provider with certificate of disposal.
- Neither the full contents of any track of the magnetic stripe nor the three-digit card validation code may be stored in a database, log file, electronic document or point of sale product.

c. Third-Party Vendors (Processors Software Providers Payment Gateways or Other Service Providers)

- Financial Services must approve each merchant bank or processing contract of any third-party vendor that is engaged in, or proposes to engage in, the processing or storage of transaction data on behalf of the University—regardless of the manner or duration of such activities.
- Financial Services must ensure that all third-party vendors adhere to all rules and regulations governing cardholder information security.
- Financial Services must contractually require that all third parties involved in credit card transactions meet all PCI security standards, and that they provide proof of compliance and efforts at maintaining ongoing compliance.
- Information must be maintained about which PCI-DSS requirements are managed by each third-party provider and which are managed by Financial Services.

d. Additional Requirements

- Complete an annual self-assessment-both at the Department and University level. (Self-Assessment documents will be available for departments.) The PCI Compliance Coordinator will schedule annual assessments.
- Without adherence to the PCI-DSS standards, the University would be in a position of unnecessary reputational risk and financial liability. Merchant account holders who fail to comply are subject to:
  - Any fines imposed by the payment card industry
  - Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees
  - Suspension of the merchant account
- Self-Assessment
  - The PCI Compliance Coordinator will notify each Department ahead of the time-line to complete and submit the annual departmental assessment. This assessment is the responsibility of the PCI Department Coordinator.
  - The PCI-DSS Self-Assessment Questionnaire must be completed at the University level by the merchant account owner annually and anytime a credit card related system or process changes.
- Training
  - Annual employee training programs must be offered to train employees on PCI DSS and the importance of compliance. This will be made available by the Financial Data Manager and coordinated by the PCI Compliance Coordinator. PCI Department Coordinators must ensure that employees with access to card data within their departments take part in annual PCI training and that all new employees within these departments take part in PCI training upon hiring.

8. Responsible Organization/Party:

The AVP Financial Services has the responsibility for notifying the applicable Department Heads and Data Managers about changes to the policy. S/he will be assisted by the CIO, and

the Financial Projects Manager.

9. Enforcement:

The AVP Financial Services will oversee enforcement of the policy. Additionally this individual will investigate any reported violations of this policy, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the policy. S/he will be assisted by the CIO, Financial Projects Manager as well as other University Officers as needed.

10. Additional Resources

PCI DSS Requirements and Security Assessment Procedures:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI DSS Quick Reference Guide Version 3.0
https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf

---

Review Period: 7 years;
Date for Next Review: 2023-2024;
Related Policies and Procedures: To be determined;
Policy Superseded by this Policy: None.

The University Secretariat manages the development of policies through an impartial, fair governance process, and in accordance with the Policy Governance Framework. Please contact the University Secretariat for additional information on University policies and procedures and/or if you require this information in another format:

Open: Monday through Friday from 8:30am to 4:30pm;
Location: University Centre, Thunder Bay Campus, Room UC2002;
Phone: 807-346-7929 or Email: univsec@lakeheadu.ca.