The University of Western Ontario
Unit PCI Self-Assessment Questionnaire

Unit: _____ Date: _____

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive standard that was developed by the PCI Council (https://www.pcisecuritystandards.org/index.shtml) with the intention of helping organizations proactively protect cardholder data (CHD). All merchants who process, store and/or transmit cardholder data must be compliant with the requirements of the most current version of PCI DSS, their Merchant Account Agreement and Card Brand Rules and Regulations.

The Bank Card Committee has developed a number of effective practices for protecting cardholder data in Western's environment. Please review these practices and indicate if they have been implemented in your unit. If they have not, please indicate what your unit is doing that would achieve the same result.

Employee Awareness

Employees must be knowledgeable about how to process, transmit and store cardholder data and must be aware of the sensitivity of cardholder data. In particular, the credit card number, card verification code, card expiry date and cardholder name comprise information that must be protected at all times. Employees must understand that they are responsible for holding cardholder data in confidence and that it should only be disclosed for a required business purpose.

Unit leaders must know their bank card processes and be aware of their employees and their backgrounds. Unit leaders and/or hiring managers must complete the appropriate level of background investigation prior to hiring potential candidates that will have access to cardholder data. Unit leaders and employees who process, transmit and/or store cardholder data must be aware of and abide by the following policies and procedures:

Bank Card Policy - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp129.pdf

Code of Behavior for Use of Computing Resources and Corporate Data - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113.pdf

Procedure for Code of Behavior for Use of Computing Resources and Corporate Data - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113_procedure.pdf

Finance, Information Technology, and Internal Audit Bank Card Codes of Procedure - http://commerce.uwo.ca/codes_of_procedure/index.html

Western Security Breach Protocol - http://commerce.uwo.ca/security_breach_plan/index.html

Training for bank card processing must be completed by all new employees and at least annually to existing employees.

Unit leaders are responsible for ensuring the breach protocol is displayed for employees in areas where cardholder data is processed, transmitted or stored and that employees know the first point of contact in the instance of a suspected breach. If a unit leader knows or suspects that cardholder data has been compromised or that a point-of-sale (POS) device has been tampered with, the incident must be reported using the Western's Security Breach Protocol.

OBJECTIVE	**N/A**	**YES**	**NO**, If no then explain how the objective will be achieved.
Training for bank card processing and protecting cardholder data is completed by all new employees and to all employees at least annually.			
Employees who process bank card transactions have read and abide by the policies and procedures listed above.			
Unit leaders are familiar with employees who process bank card transactions and/or have access to cardholder data.			
Employees are aware of Western's Security Breach Protocol and understand how to report a potential bank card breach.			

Protecting Cardholder Data

Cardholder data can be received through several channels. Card present transactions are the most secure method to receive payment.

It is prohibited to store cardholder data electronically at Western University. This includes on a computer, tablet, USB drive, database, server etc. Cardholder data must be removed or properly masked before any electronic scanning is completed to archive information.

Cardholder data should only be stored (not electronically) for the minimal period of time possible to process the transaction. Cardholder data must be always kept in a secure location (i.e., in a locked cabinet, inside of a locked room.) Access to this information must be limited to those who require the cardholder data for business purposes. Keep cardholder data storage to a minimum by implementing data retention and disposal policies.

All cardholder data that is stored must be inventoried. This log should include the card type, cardholder name, last four digits of the personal account number (PAN) and a contact number. This inventory is to ensure that Merchants can easily determine the cardholder data that is missing in the event of a breach. This inventory must **not** contain the full PAN, the expiration date, or the card verification code. If requested, a Western Merchant must be able to produce an inventory log of stored card holder data.

Forms should be designed to allow the removal of the credit card number, verification number and expiry date (i.e., at the bottom of the form) after the payment has been processed. The three- or four-digit verification code can only be requested if it is necessary to complete a card not present transaction. This code cannot be retained after the authorization of payment.

Electronic media (e-mail, text messaging, etc.) is not a secure method to send or receive cardholder data and is strictly prohibited as a means of accepting cardholder data. If cardholder data is received via e-mail, it must be deleted from both the inbox and deleted items folder. The trash folder must be purged. If you reply to an e-mail containing cardholder data, this information must be removed. Transactions where cardholder data is received via electronic media must **not** be processed.

A network connected fax machine and voicemail are considered electronic media. Any cardholder data received via these methods must also be destroyed. Using cardholder data received by voicemail is strictly prohibited.

Cardholder data should not be accepted over Western campus telephones (VoIP telephones and Jabber). VoIP traffic containing cardholder data is in scope for applicable PCI DSS controls wherever that traffic is stored, processed or transmitted internally over an entity's network. Western VoIP traffic is not secured and there is risk of unauthorized internal and external access.

If cardholder data is transported from one location to another it must be treated like cash. The number of receipts or forms and total value of the transactions should be recorded and signed by an employee. The information should be placed in a sealed envelope or deposit bag for transportation. The receiving area must verify the number and total value of receipts and sign for acceptance. Like cash, cardholder data must never be left unattended. It must be secured at all times.

Western Archives is a secure, confidential storage location for records that are not required for operational purposes but are needed to satisfy audit requirements.

Cardholder data that is no longer required must be destroyed using a crosscut shredder or through Western's preferred shredding service provider.

OBJECTIVE	**N/A**	**YES**	**NO**, If no then explain how the objective will be achieved.
Cardholder data, including the card verification codes, are not stored electronically.			
Cardholder data is not transmitted electronically (i.e., e-mail, text messaging, network connected fax machine, voicemail, etc.)			
Cardholder data is not accepted over Western Campus telephones.			

OBJECTIVE	N/A	YES	**NO**, If no then explain how the objective will be achieved.
Paper-based cardholder data is stored in a secure location with limited access and always protected.			
Stored cardholder data is inventoried.			
Unit has a cardholder data retention policy.			
Cardholder data which is no longer needed for business purposes is destroyed using a cross-cut shredder or through Western's preferred shredding service provider.			

Processing Bank Card Transactions

The ability to process bank card transactions through any payment system (including point-of-sale devices) and access to cardholder data must be limited to those individuals whose job requires such access.

Access to payment systems must be limited to those individuals whose job requires such access for business purposes. Assign access based on individual personnel's job classification and function. All vendor supplied default passwords to payment systems must be changed and properly protected.

The merchant cannot discriminate against a method of payment that it has agreed to accept. For example, the merchant must offer chip and pin technology if the merchant accepts bank card payments through a point-of-sale device.

All point-of-sale devices must be inspected on a daily basis, at minimum. This must be done with the Interac or Moneris *Point of Purchase Integrity Checklist* (http://commerce.uwo.ca/documentation/index.html.) If requested, a Western Merchant must be able to produce an inspection log for their POS devices. All employees who operate POS devices must be properly trained, including training on how to detect if a POS device has been tampered with and what to do if they suspect that a POS device has been tampered with.

If you process transactions using POS devices:

- All POS devices (except Long-range cellular devices) must be placed in the dedicated PCI VLAN (if you are unsure if your device is in the PCI VLAN, please contact the Security Operations Center at security@uwo.ca);
- Maintain an up-to-date list of devices, including make, model of device, location of device and serial number
- Your device(s) must be secured and protected at all times;
- Always change vendor-supplied defaults.
- Disable WIFI, Bluetooth and all unnecessary functionalities.
- You must provide training for personnel to be aware of attempted tampering or replacement of devices;
- You must complete the Interac or Moneris *Point of Purchase Integrity Checklist* daily (at minimum);
- Assign responsibility and maintain a sign-out/sign-in procedure for long-range cellular devices. Ensure a separate individual (or supervisor) confirms the device has been returned
- SIM cards may only be used in the long-range cellular device in which it is installed and in no other wireless device and may only be used in connection with the Card processing services that Moneris is providing to you.

Merchants must never enter card holder data into a webpage, application or ecommerce solution on behalf of a customer (unless approved by the Bank Card Committee). Merchants should direct all customers to their website, applications, or ecommerce solutions to enter credit card data to complete payment. This is a PCI DSS requirement. This does not pertain to POS devices. Merchants processing payments manually through a POS device remains a PCI compliant practice.

OBJECTIVE	N/A	YES	**NO**, If no then explain how the objective will be achieved.
Card present transactions are processed immediately with the customer present using a POS device.			
Credit card payments are not entered by Western staff directly into the payment system on behalf of our customers.			

Card holder data received by Western phone system, voicemail and/or email are never processed.			
Card holder data received on forms are removed and shredded after processing.			
You have disabled WIFI, Bluetooth and all unnecessary functionalities on each POS device.			
The Interac or Moneris *Point of Purchase Integrity Checklist* is completed daily for each POS device (at minimum).			
You have a sign-out/sign-in procedure for long-range cellular devices			

Processing Bank Card Transactions: webpages, applications, or ecommerce solutions

Any web server hosted on campus or operated in "the cloud" by a department, faculty, ancillary area of Western University, or a third-party vendor on behalf of said Western departments, that engages in the use of cardholder data for any type of financial transaction is defined as an ecommerce server and is considered in-scope of our PCI cardholder data environment (CDE). These servers must adhere to the following PCI-DSS requirements.

1. All vendor-supplied defaults must be changed. (This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.)
    a. All unnecessary default accounts must be removed or disabled.

2. All system components (e.g., Operating System, Hardware Bios, Virtual Hosting environment, web server software etc.) must be protected from vulnerabilities by applying all vendor supplied security patches within one month of release.

3. All users must be assigned a unique ID before allowing them to access system components or cardholder data.
    a. Access for any terminated users must be removed or deactivated immediately;
    b. User accounts must be protected by at least one of these methods of authentication:
        i. Something you know, such as a password or passphrase;
        ii. Something you have, such as a token device or smart card;
        iii. Something you are, such as a biometric.

4. All system and user passwords/passphrases must:
    a. Be a minimum length of at least eight characters;
    b. Contain both numeric and alphabetic characters;
    c. Contain at least one special character; and
    d. Contain both upper- and lower-case alphabetic characters.

5. No system will be permitted to use generic or shared user or system IDs.

6. All system components must be "Hardened" against exploit.
    a. All hardening activities must be documented.

OBJECTIVE	**N/A**	**YES**	**NO**, If no then explain how the objective will be achieved.
All vendor-supplied defaults have been changed.			
All systems are patched on a regular basis, no longer than one month of patch release.			
All users are assigned their own unique ID, and no generic or shared IDs exist.			
Access for terminated users has been removed or deactivated			
All passwords meet the complexity requirements noted above.			
System hardening guidelines have been applied and documented.			

3rd Party Service Providers

Merchants that use 3rd party service providers must understand the type of vendor they are working with and ensure the vendor has taken appropriate steps to protect card holder data.
Merchants should:

- Go through the TRAC (Technology Risk Assessment Committee) process before using 3rd party service providers/applications.
- Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data. This includes ecommerce sites with service providers.
- Maintain a list of service providers including a description of the service provided.
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
- Monitor service providers PCI DSS compliance status at least annually by obtaining and keeping on file the Attestation of Compliance (AOC).
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the merchant by obtaining the PCI Responsibility Matrix from the service provider.
- For all service providers involved in the payment process understand your responsibilities.
- Provide all the above to the Bank Card Committee for the annual PCI Compliance audit or upon request.

OBJECTIVE	**N/A**	**YES**	**NO**, If no then explain how the objective will be achieved.
Maintain a list of service providers including a description of the service provided.			
Current contracts for all service providers are on file.			
AOCs are on file for all service providers.			
PCI Responsibility Matrix obtained and reviewed for all service providers.			

To the best of my knowledge and belief, I confirm I have read, understood and answered the above completely and accurately.

_____
Budget Unit Head

_____ _____
Signature Date

Please sign and return to the Bank Card Committee, c/o Lin Cui, Room 6120, Support Services Building

The University of Western Ontario
Inventory of Point-of-Sale Devices

Unit: _____ Date: _____

For units with point-of-sale devices, please list them below.

Merchant Account Number	Model Number	Serial Number	IP Address	Location (Building and Room Number)

The University of Western Ontario
Inventory of Ecommerce sites

Unit: _____ Date: _____

For units hosting any ecommerce sites, please list them below.

Merchant Account Number	Moneris Store ID	URL of Redirect to Moneris	Web Page Integration Type - Hosted Pay Page, MCO (Moneris Checkout) or Hosted Tokenization	Web Page Third Party Service Provider or Hosted Application (if applicable)

Note: Contact security@uwo.ca if you have any questions regarding the completion of this chart.

The University of Western Ontario
Information Security Policy Attestation

Unit: _____ Date: _____

By signing below, the employee, who processes bank card transactions, confirms that they have read and understand the University's information security polices:

Bank Card Policy - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp129.pdf

Code of Behavior for Use of Computing Resources and Corporate Data - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113.pdf

Procedure for Code of Behavior for Use of Computing Resources and Corporate Data - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113_procedure.pdf

Finance, Information Technology and Internal Audit Bank Card Codes of Procedure - http://commerce.uwo.ca/codes_of_procedure/index.html

Western Security Breach Protocol - http://commerce.uwo.ca/security_breach_plan/index.html

EMPLOYEE NAME	POSITION	SIGNATURE