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. All merchants who process bank card transactions must be compliant with the requirements of the most current version of PCI DSS, their Merchant 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 and store bank card transactions 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 to hold cardholder data in confidence at all times 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 employees who process bank card transactions 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
Computing Resources Security - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp120.pdf
Finance, Information Technology and Internal Audit Codes of Procedure - http://commerce.uwo.ca/cop.html
Western Security Breach Protocol - http://commerce.uwo.ca/pdfs/PCI_INCIDENT_PROCESS_FLOW_V1.5.pdf

Training for bank card processing must be provided to all new employees and at least annually to existing employees. Training material is available on the commerce website (http://commerce.uwo.ca/index.html).

If a unit leader knows or suspects that cardholder data has been compromised or that a point of sale 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 provided to 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 including in-person, over the telephone and fillable forms. 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, database or server. Cardholder data must be removed or properly masked before any electronic scanning is completed to archive information.

Cardholder data should only be stored for the minimal period of time possible to process the transaction. Cardholder data must be kept in a secure location at all times (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.

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.

Fax machines may only be used to receive cardholder data if the machine is connected using an analog phone line. If the fax machine is connected through a network connection, it is considered electronic media and prohibited as a means of accepting cardholder data.

Voicemail is also considered electronic media. If you receive cardholder data via voicemail the message must be deleted immediately. Storing cardholder data on voicemail is strictly prohibited.

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 should verify the number and total value of receipts and sign for acceptance. Like cash, cardholder data should never be left unattended. It must be secured at all times.

Western Archives is considered to be 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 Eco-Shred program.

OBJECTIVE	**N/A**	**YES**	**NO**, If no then explain how the objective will be achieved.
Credit card numbers including the card-validation codes are not stored on any computer, database or server.			
Cardholder data is not transmitted electronically (i.e. e-mail, text messaging or network connected fax machine.)			
Paper based Credit card payment information is stored in a secure location with limited access and protected at all times.			
Unit has a credit card retention policy.			
Cardholder data which is no longer needed for business purposes is destroyed using a cross-cut shredder or through Western's Eco-Shred program.			

Processing Bank Card Transactions

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

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 terminal.

Access to payment systems must be limited to those individuals whose job requires such access for business purposes. All vendor supplied default passwords to payment systems must be changed and properly protected.

If you process transactions using point of sale (POS) terminals:

- All POS terminals must be placed in the dedicated PCI VLAN (if you are unsure if your device is in the PCI VLAN, please contact the Network Operations Center);
- Your terminal(s) must be secured and protected at all times;
- You must provide training for personnel to be aware of attempted tampering or replacement of devices;
- You must regularly inspect the devices to ensure the device has not been tampered with or replaced;
- The use of long range wireless POS devices at Western University is prohibited.

Units that use POS terminals should implement practices to prevent tampering with these devices as suggested in the *Recommended Checklist* documents located at: http://www.commerce.uwo.ca/documentation.html.

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 either a POS terminal or manually entered into a payment system.			
Credit card payments received over the telephone are entered directly into the system while the customer is on the telephone. Cardholder data must not be stored in voicemail.			
Credit card numbers received on forms are removed and shredded after processing.			
Credit card receipts do not display all digits of the credit card number.			
Effective practices relating to POS devices have been implemented as detailed in the POS Checklist.			

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 Justin Riedstra, Room 6120, Support Services Building

The University of Western Ontario
Inventory of Point of Sale Terminals

Unit: _____ Date: _____

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

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

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
Commerce Codes of Procedure - http://commerce.uwo.ca/cop.html
Code of Behavior for Use of Computing Resources and Corporate Data – http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp113.pdf
Computing Resources Security - http://www.uwo.ca/univsec/pdf/policies_procedures/section1/mapp120.pdf
Western Security Breach Protocol - http://commerce.uwo.ca/pdfs/PCI_INCIDENT_PROCESS_FLOW_V1.5.pdf

EMPLOYEE NAME	POSITION	SIGNATURE