Policy



**Title:** PCI Compliance

**Effective Date:** 01/01/18

**Applies to:** University Wide

**Statement:**

The Western University Financial Services and Treasury (UFS&T) is committed to compliance with the Payment Card Industry (PCI) Data Security Standard, a standard adopted internationally by the major credit card brands (e.g., Visa, MasterCard, Discover, and American Express) to protect credit card data, regardless of where that data is processed or stored (“PCI Standard”).

**Purpose**:

To ensure the University is compliant to the PCI Standard the UFS&T department is responsible for the implementation and oversight of this policy and the general practice in which the University employees handle credit card data, including:

* Establishing and closing merchant accounts. A merchant account is a type of bank account that allows businesses to accept payments by debit or credit cards;
* Establishing and maintaining relationships with the credit card payment processing providers and issuing banks;
* Approving any Point of Sale (POS) device or system to be used within the university;
* Defining the methods of transacting online payments on behalf of the university;
* Engaging a PCI Qualified Security Assessor, in consultation with Office of Compliance;
* Maintaining an inventory of all WesternU departments that process credit card transactions using a WesternU approved merchant account;
* Coordinating with IT, as necessary, to review network segmentation configurations and other technical safeguards;
* Coordinating with the Office of Compliance to monitor and audit compliance with this policy;
* PCI training/education;
* Enforcement of this policy and the PCI Standard including immediate suspension or termination of the ability to process or store credit cards if a department fails to comply with this policy or the PCI Standard; and
* Other duties related to PCI Compliance as determined by the University.

Failure to comply with PCI Standard’s policy and its procedure may result in revocation of a department’s merchant account.

**Departments processing credit cards** – all departments that accept credit/debit cards must protect credit card data in compliance with this policy and the PCI Standard. All departments that process credit/debit data will implement the business standards described in Appendix D of this policy.

Departments that processed credit cards prior to the effective date of this policy must be in full compliance with the policy and the PCI Standard within 60 calendar days of policy issue date in order to continue to process credit/debit cards (See Appendix A).

**IT Department** – is responsible for:

* approving network segmentation configurations performed in compliance with this policy and the PCI Standard in conjunction with Treasury Services;
* assisting departments with network segmentation configuration;
* providing certain security information and event management functions;
* conducting appropriate vulnerability scanning of WesternU systems that transmit, generate or otherwise access credit/debit card information;
* initiating investigations relating to security incidents; and
* Performing other monitoring and reviews of computer and/or computer networks to ensure that security features are in place and are adequate to protect credit/debit card data.

**Procedures**

For comprehensive procedures involving establishing and maintaining merchant accounts (POS systems), refer to Appendix A-D and the PCI Pre-Qualification form.

**Third Party Vendor Risk Management**

Any third-party vendor that processes, transmits, generates, stores or otherwise accesses credit/debit card data on Western University’s behalf must work with University Financial Services and Treasury to initiate this process.

Before Purchasing executes an agreement with a vendor, the department should request a copy of the vendor’s most current report on compliance (“ROC”) or attestation of compliance (“AOC”) for the specific services being provided to the university. In addition, the department is required to monitor the vendors’ PCI Standard compliance status at least annually and submit them to the UFS&T.

**Incident Response Plan**

A “security breach” is an unauthorized acquisition of data that compromises the security, confidentiality or integrity of information maintained by WesternU and covered under this policy. This includes breaches that involve physical security as well as computer or information systems security and also could include unauthorized access to WesternU wireless services. Any university employee aware of an actual or suspected information security breach must report it immediately to his/her respective manager and the WesternU IT Department.

IT and the University Compliance Office shall lead the incident response team for suspected or confirmed breaches of the PCI Standard. The team also includes representatives from the UFS&T.

Depending on the incident, WesternU may have an obligation under state and/or federal law to notify the individuals whose information were breached as well as the applicable state or federal oversight agencies. The Office of Compliance will manage the university’s response and prepare and submit any notifications as required or appropriate, in coordination with IT and incident response team.

Departments may not conduct their own investigation without first consulting and coordinating with IT and the University Compliance Office. Further details about the incident response process are included in Appendix C.

**Resources:**

[**www.pcisecuritystandards.org**](http://www.pcisecuritystandards.org)

**Forms:**

**[PCI Pre-Qualification Form](G:\\isampson\\Updated Policies for Chris\\PCI Compliance Policy and Attachments\\PCI-Pre-Qualification-Form.doc)**

**Appendices:**

**[Appendix A – PCI Security Safeguards](G:\\isampson\\Updated Policies for Chris\\PCI Compliance Policy and Attachments\\Appendix A of PCI DDS.doc)**

[**Appendix B – Procedures**](file:///G:\isampson\Updated%20Policies%20for%20Chris\PCI%20Compliance%20Policy%20and%20Attachments\Appendix%20B%20of%20PCI%20DDS.doc)

**[Appendix C – PCI Incident Response Plan](G:\\isampson\\Updated Policies for Chris\\PCI Compliance Policy and Attachments\\Appendix C of PCI DDS.doc)**

[**Appendix D – Business Standards**](file:///G:\isampson\Updated%20Policies%20for%20Chris\PCI%20Compliance%20Policy%20and%20Attachments\Appendix%20D%20of%20PCI%20DDS.doc)

**Responsible Offices:**

**University Financial Services and Treasury**

[**raldama@westernu.edu**](mailto:raldama@westernu.edu)  
(909) 706-3514

**Information Technology**

**TechSupport@westernu.edu**

(909) 469-5432

**Office of Compliance**

[**trich@westernu.edu**](mailto:trich@westernu.edu)  
(909) 706-3871

**Issued by**

Rosa Aldama

**Key Words:** Credit Card Security Merchant

**Responsible Department:** University Financial Services & Treasury

**Contact:** Rosa Aldama

**Title:** Financial Accountant

**Email:** raldama@westernu.edu

**Origination Date:**  01/01/2018

**Review Date:**  06/01/2020