Roger William's University

PCI Compliance Policy

Purpose

This policy is 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 Payment Card Industry Data Security Standard ("PCI-DSS") requirements as established by the PCI Security Standards Council ("PCI SSC"). Without adherence to the PCI-DSS standards, the university would be in a position of unnecessary reputational risk and financial liability.

The PCI-DSS, is a worldwide security standard assembled by the PCI SSC. The 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 threats. The standards apply to all organizations that store, process, or transmit cardholder data.

Scope of Policy

This policy applies to all university departments that collect, maintain, or have access to credit card information as well as third party vendors that process and store credit card information for the university using the university's merchant accounts.

All persons who have access to credit card information, including:

- Every employee that accesses, handles, or maintains credit card information.
- Employees who contract with third party vendors who process credit card payments on behalf of the university.
- IT staff responsible for scanning the university systems to ensure that no credit card numbers are stored electronically.

Policy

The university requires compliance with PCI standards. To achieve compliance, the following requirements must be met by departments accepting credit cards to process payments on behalf of the university.

General Requirements

- Credit card merchant accounts must be approved by the Vice President of Accounting and Treasury Management.
- All employees who have access to credit card information must be familiar with and adhere to this policy.
- The Vice President for Accounting & Treasury Management and Chief Information Officer will complete an annual self-assessment questionnaire and attestation of compliance following the PCI-DDS requirements.

Storage and Disposal

- Credit card information must not be entered/stored on university network servers, workstations, laptops, smartphones, or other electronic devices.
- Credit card information must not be transmitted via email.
- Web payments must be processed using a PCI-compliant service provider approved by the Vice President for Accounting and Treasury Management. Credit card numbers must NOT be entered into a web page of a server hosted on the RWU network.
- Although electronic storage of credit card data is prohibited by this policy, the university will perform a quarterly network scan to ensure that the policy has not been violated.
- Any paper documents containing credit card information should be limited to only information required to transact business, only those individuals who have a business need to have access, should be in a secure location, and must be destroyed via approved methods 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.
- Securely dispose of sensitive cardholder data 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 shredding either in-house or with a third-party provider with certificate of disposal.
- Neither the full contents of any track for the magnetic strip nor the three-digit card validation code may be stored in a database, log file, or point of sale product.

Third Party Vendors (Processors, Software Providers, Payment Gateways, or Other Service Providers

- The VP for Accounting and Treasury Management must approve each merchant bank or processing contact of any third-party vendor that is engaged in, or propose to engage in, the processing or storage of transaction data on behalf of RWU—regardless of the manner or duration of such activities.
- Ensure that all third-party vendors adhere to all rules and regulations governing cardholder information security using such methods as obtaining an annual PCI report attesting to PCI scan compliance and an Independent Auditors report on Statements on Standards for Attestation Examinations ("SSAE 16").
- 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.

Further Guidance

Questions: The university recognizes that this policy will not address all circumstances. Specific questions not answered by this Policy should be addressed to:

Gloria Arcia, VP for Accounting and Treasury Management

- Office: Admin 201
- Phone: 401-254-3843

Daryl Ford, Chief Information Officer

- Office: Law School
- Phone: 401-254-3148

Standard Number: IT.PCI.V1
Category: Payment Card Security
Owner: Information Technology
Effective: TBD
Revision History: 8/18/2021 Security Advisory Group
Review Date: 12/19/2024
(X) Applies to University, Including Law School
( ) Applies to University, Except Law School
Policy No. PCI2019