Policy

The purpose of this policy is to establish a framework for processing payment cards to prevent loss or disclosure of cardholder data.

This policy governs payment card handling, processing, transmission, storage and disposal of cardholder data transactions for all departments accepting credit card payments for goods and services.

Departments wishing to accept credit card payments must comply with the Payment Card Industry Data Security Standards (PCI-DSS) established by the payment card industry and are based on best practices in data security. Compliance with PCI standards protects the University’s students, customers, and employees.

This policy defines the steps that departments accepting credit cards must use to access and secure payment card data in their business processes as well as acceptable technology.

The University’s PCI Team, comprised of Business Services and IT staff, has been charged with administrative oversight of campus payment card merchants and adherence to this policy.

Definition of Terms

Cardholder: The person to whom a payment card is issued or any individual authorized to use the payment card.

Cardholder Data: At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

High Risk Data: Any data where the unauthorized disclosure, alteration, loss, or destruction may: cause personal or institutional financial loss, or the unauthorized release of which would be a violation of a statute, act or law; constitute a violation of confidentiality agreed to as a condition of possessing or producing or transmitting data; cause significant reputational harm to the University; or require the UW System to self-report to the government and/or provide public notice if the data is inappropriately accessed.

Institution: University of Wisconsin – River Falls.

Merchant Account: A bank account that enables the holder to accept credit cards for payment.

Merchant Department: Any department or unit (can be a group of departments or a subset of a department) which has been approved by the Controller’s Office to accept payment cards.
**Payment Card:** A financial transaction card (credit, debit, etc.) issued by a financial institution; also called Bankcard/Payment Card/Charge Card/Credit Card/Debit Card.

**Payment Card Industry Data Security Standards (PCI DSS):** A multifaceted security standard developed and owned by the major payment card companies that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. PCI DSS represents a common set of tools and measurements to help ensure the safe handling of sensitive information. The standard is comprised of 12 requirements that are organized in 6 logically related groups or “control objectives.” Failure to conform to these standards can result in losing the ability to process payment card payments and being audited and/or fined.

**P2PE:** A comprehensive set of security requirements for point-to-point encryption solution providers, this PCI standard helps those solution providers validate their work. Using an approved point-to-point encryption solution will help merchants to reduce the value of stolen cardholder data because it will be unreadable to an unauthorized party. Solutions based on this standard also may help reduce the scope of their cardholder data environment – and make compliance easier.

**Sensitive Authentication Data:** Security-related information (including but not limited to card validation codes/values, full track data from the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

**Service Provider:** A business entity that is not a payment brand but is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This includes companies that provide services that control or could impact the security of cardholder data. Examples include service providers that provide managed firewalls, intrusion detection systems (IDS), and other services.

**Procedure**

Merchant departments at UW-River Falls that accept payment cards are required to do so in accordance with PCI DSS; UW System Administrative Policy 350, *Payment Card Compliance Policy*, and the following procedures. Information protected from unauthorized disclosure by the PCI DSS is classified by the UW System as High Risk data, per *UW System Administrative Procedure 1031.A, Information Security: Data Classification*.

**A. Card Acceptance and Handling**

The opening of a new merchant account for accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card in that department will be charged to the individual merchant.

1.1. Interested departments or merchants should contact the University of Wisconsin-River Falls Controller’s Office to begin the process of accepting payment cards. Steps include:

   1.1.1. Completion of a New Merchant Application Form available from the Accounting Services website
   1.1.2. Completion of training
   1.1.3. Review and acknowledgement of the UW System Administrative Policy 350, *Payment Card Compliance Policy*, including proof of ongoing compliance with all requirements of the policy
1.2. Any department accepting payment cards on behalf of the institution must designate an individual within the department who will have primary authority and responsibility within that department for oversight of payment card transactions. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the primary is unavailable.

1.3. Specific details regarding daily processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Detailed instructions (for equipment use, daily terminal close out, completing a deposit slip, etc.) will be provided to the Merchant when the merchant account is established and are also available by contacting the Student Billing office.

1.4. All service providers and third-party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all service providers and:

1.4.1. Ensure contracts include language stating that the service provider or third-party vendor is PCI DSS compliant and will protect all cardholder data.

1.4.2. Annually verify the PCI DSS compliance status of all service providers and third-party vendors. A lapse in PCI DSS compliance could result in the termination of the relationship.

1.5. Departments will be responsible for any charges associated with ongoing maintenance of their accounts including equipment rental or purchases, processing charges, technology upgrades or other credit card related materials. Some payment applications may require additional knowledge that is not on staff within the University and/or external assessment consulting hours may be required to implement and validate payment applications, those fees will be assessed on the merchant.

1.6. Upon approval of a merchant account, the “primary authority of the department” and the “person of secondary responsibility” will be expected to provide a signed written acknowledgment of the UWSA Policy 350, these “Payment Card Procedures” and the PCI Self-Assessment Questionnaire (SAQ) associated with their account. A template will be provided to the individual from the Student Billing office.

B. Payment Card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

I. Processing and Collection

2.1. Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list periodically to ensure that the list reflects the most current access needed and granted.

2.2. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:
2.2.1. Maintaining an inventory/list of devices and their location;
2.2.2. Periodically inspecting the devices to check for tampering or substitution;
2.2.3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

2.3. Email must never be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. If it does occur, disposal as outlined below is critical. If payment card data is received in an email then:

2.3.1. The email should be replied to immediately with the payment card number deleted stating that, “The University of Wisconsin-River Falls does not accept payment card data via email as it is not a secure method of transmitting cardholder data”.
2.3.2. Provide a list of the alternate, compliant option(s) for payment.
2.3.3. Delete the email from your inbox and delete it from your email Trash.

2.4. Fax machines and Cisco Voice Over IP telephones shall not be used to transmit or receive payment card information to a merchant department.

2.5. Public kiosks will not be permitted for acceptance of payment cards. i.e. providing a computer in an office to complete an online process involved with a credit card.

2.6. A mixed-use computer workstation (tablet, or other device) will not be permitted for administrative uses where card holder data is processed, i.e. to setup monthly recurring transactions or to process sale transactions on behalf of a customer in person or mail. (A mixed used computer is a standard workstation used for email, etc.) A dedicated workstation must be procured by Technology Services and established on a dedicated network.

II. Storage and Destruction

3.1. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

3.2. Physical security controls are in place to prevent unauthorized individuals from gaining access to the electronics devices, buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data. A surveillance camera or electronic door access should be installed, as appropriate, to protect long-term storage of the card holder data. (Contact Police Chief to initiate review.)

3.3. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, chip, NFC or the card validation code.

3.4. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, tablets, smartphones, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

3.5. Cardholder data should not be retained any longer than that defined by a legitimate business need. CHD must be destroyed immediately following the required retention period using a PCI DSS-approved method of destruction. Costs associated with the procurement of a compliant method is the responsibility of the department.
3.6. The UW System defined maximum period of time that credit card receipts and/or deposit transactions documents may be retained is three years from the date of transaction, unless a longer retention time period is required by contract or law. The maximum period of time that PCI Operator Training forms and corresponding PCI Compliance Logs may be retained is three years from the date of creation. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the required retention period. For more detail regarding record retention, please see the University of Wisconsin System Fiscal and Accounting General Records Schedule.

C. Risk Assessment

Implement a formal risk assessment process in which current threats and vulnerabilities to the institution’s network and processing environment, including staff, are analyzed. Risk assessments must be conducted annually and must commence no later than two years after the initial adoption of UW System Administrative Policy 350, Payment Card Policy. The Division of Technology Services will procure on behalf of the merchants a risk assessment of the infrastructure and threats; departments that accept payment cards should also conduct an assessment of their physical environments and assess risks to the payment environment. Address all threats with mitigation tasks, timelines, and/or acceptance statements. Prepare and maintain documented output from the risk assessment exercise(s). Costs associated with the risk assessment will be spread across the merchant accounts as an assessed fee.

D. Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute the University of Wisconsin-River Falls’ response plan. This plan must meet or exceed the requirements of UW System Administrative Policy 1033, Information Security: Incident Response and should be reviewed at least annually.

If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify per the University of Wisconsin-River Falls’ response plan.

E. Policy and Training

Ensure policy and procedure documentation governing cardholder data exists and that it covers the entirety of the PCI DSS. Document users’ acknowledgement of understanding and compliance with all policies and procedures annually. Ensure training on the PCI DSS and overall information security is provided to all staff members with access to cardholder data and/or the processing environment upon hire, and at least annually thereafter.

Authority

The UW-River Falls Chancellor approves this policy in accordance with the Administrative Policy process. The Vice Chancellor for Business and Finance is responsible for the substance of, and compliance with all administrative policies. The Policy Owner (Responsible Office) is responsible for the administration and maintenance of this policy. Request an exception to this policy by writing to administrative-policy@uwrf.edu.
Sanctions and Appeals Process
Failure to adhere to the provisions of this policy may result in a department losing the privilege of accepting credit cards as form of payment. Individuals found to be negligent may result in appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff, and/or civil or criminal prosecution.

University Responsibilities
Department/Unit accepting credit cards

Background
UW-River Falls is committed to safeguarding personal and account information conveyed in processing debit and credit card payments. Also, the privilege of accepting payment cards from the leading card brands depends upon compliance with specified security standards. To comply with these standards, it is the policy of UW-River Falls that security standards relating to payment card transactions be specified and applied.

Related Documents
UW System Administrative Policy 350, Payment Card Compliance Policy
Division of Technology Services - Incident Response Plan
PCI DSS Quick Reference Guide

Contact
Please direct questions about this policy to administrative-policy@uwrf.edu.