**[Institution logo here]**

Payment Card Procedures Template

## [UW System Administrative Policy 350, Payment Card Policy](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/payment-card-compliance-policy/)*,* requires that all UW System institutions develop procedures to prevent loss or disclosure of cardholder data. Below is a template that UW System institutions are encouraged to use when developing their institutional procedures.

## Purpose of Procedures

The purpose of these procedures is to prevent loss or disclosure of cardholder data (CHD) in accordance with [University of Wisconsin System Administrative Policy 350, Payment Card Policy](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/payment-card-compliance-policy/).

## Responsible Institutional Officer

[**Title of position responsible for ensuring compliance with and maintenance of these procedures]**

## Definitions

**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:** Includes all UW System universities, campuses, and UW System Administration.

**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 a UW System institution 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.

**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.

## Procedures

Departments at **[Institution Name]** 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.](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/information-security-data-classification/)

### 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. Interested departments or merchants should contact the **[Institution Name’s]** payment coordinator to begin the process of accepting payment cards. Steps include:
		1. Completion of an “Application to become a Merchant Department”
		2. Completion of training
		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
		4. **[If applicable]** submit application for E-commerce for approval by the E-commerce committee. The application and policy are found at **[location link].**
	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.
	3. Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the **[institution department responsible]**.
	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. Ensure contracts include language stating that the service provider or third-party vendor is PCI DSS compliant and will protect all cardholder data.
		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.

### 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.

#### Processing and Collection

* 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. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:
		1. Maintaining an inventory/list of devices and their location;
		2. Periodically inspecting the devices to check for tampering or substitution;
		3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.
	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. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email then:
		1. The email should be replied to immediately with the payment card number deleted stating that, “**[Institution Name]** does not accept payment card data via email as it is not a secure method of transmitting cardholder data".
		2. Provide a list of the alternate, compliant option(s) for payment.
		3. Delete the email from your inbox and delete it from your email Trash.
	4. Fax machines used to transmit payment card information to a merchant department must be standalone machines with appropriate physical security; receipt or transmission of payment card data using a multi-function fax machine is not permitted.

#### Storage and Destruction

* 1. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.
	2. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.
	3. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe or the card validation code.
	4. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.
	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. 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.](https://www.wisconsin.edu/general-counsel/download/public_records/records_schedules/Fiscal-and-Accounting-General-Records-Schedule-%28Amended-Nov-2012%29.pdf)

### 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*. Information Technology should conduct the 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).

### Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute **[name of institutional response plan]**. This plan must meet or exceed the requirements of [UW System Administrative Policy 1033, Information Security: Incident Response](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-incident-response/) and should be reviewed at least annually.

If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify **[Institution Name ITS Security Department]**.

###  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.

### Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation the payment card brands may assess penalties to the institution’s bank which will likely then be passed on to the institution**.** Any fines and assessments imposed will be the responsibility of the impacted merchant. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties thereafter until compliance is achieved.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, or federal laws. The **[Institution Name]** will carry out its responsibility to report such violations to the appropriate authorities.

## Related Documents

Regent Policy Document 25-5, Information Technology: Information Security
UW System Administrative Policy 350, Payment Card Compliance Policy
[UW System Administrative Policy 1110, Information Technology Acquisitions Approval](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-technology-acquisitions-approval/)
[UW System Administrative Policy 1030, Information Security: Authentication](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication-2/)UW System Administrative Procedure [1030.A, Information Security: Authentication](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/) Procedure[UW System Administrative Policy 1031, Information Security: Data Classification and Protection](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification-and-protection/)UW System Administrative Procedure [1031.A, Information Security: Data Classification](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/information-security-data-classification/)UW System Administrative Procedure [1031.B, Information Security: Data Protections](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/information-security-data-protections/)UW System Administrative Policy [1032, Information Security: Awareness](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/)UW System Administrative Policy [1033, Information Security: Incident Response](https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-incident-response/)
[Current PCI DDS Requirements and Supporting Documentation](https://www.pcisecuritystandards.org/document_library?category=pcidss&subcategory=pcidss_supporting#results)
[University of Wisconsin System Fiscal & Accounting General Records Schedule](https://www.wisconsin.edu/general-counsel/download/public_records/records_schedules/Fiscal-and-Accounting-General-Records-Schedule-%28Amended-Nov-2012%29.pdf)