INFORMATION TECHNOLOGY SERVICES
George Mason University

Payment Card Industry (PCI) Security

Document Version Number:	1.0
Document Control Number:	ITS.ITSO-STD009
Last Updated:	10/8/2025
FOIA Exempt?	No

Process Owner:

- Fiscal Services, Treasury Management
- Information Technology Services, Cybersecurity Operations

PURPOSE:

This standard supports University Policy 2110 – Payment Card Security. It provides guidance to ensure the university complies with the Payment Card Industry Data Security Standard (PCI DSS) and to prevent unauthorized disclosure of customer account data.

SCOPE:

This standard applies to all university staff, employees, students, organizations, contractors, agents, affiliates, and individuals involved with the transmission, storage (electronic or physical), or processing of payment card data, including any entities or systems that can impact the security of that data. This includes all payment card activities conducted at any university-associated location or event, and any processing conducted on behalf of the university.

RESPONSIBILITIES:

Fiscal Services: Fiscal Services is responsible for the review of practices in connection with payment card receipt transactions. Under the oversight of Fiscal Services, the merchant-level Self-Assessment Questionnaires (SAQs) and the university SAQ are maintained in CampusGuard Central (CGC). CampusGuard (vendor) is responsible for receiving all merchant-level SAQs to consolidate into a single SAQ and provide to Fiscal Services. A copy of the consolidated SAQ is to be retained in CGC. Fiscal Services and Cybersecurity Operations will partner with each other to communicate and support processes meant to ensure that merchant systems and merchant departments align with the university's compliance requirements.

Information Technology Services: Cybersecurity Operations is responsible for coordinating the university's compliance with the PCI Standard's technical requirements (e.g., Information Security Policies and Standards, annual penetration tests, vulnerability scans, and PCI DSS scope validation). Where technical control requirements are the responsibility of Information Technology Services, Cybersecurity Operations will validate that the controls are enforced. Cybersecurity Operations will provide technical control guidance on requirements to merchant departments. Additionally, it will lead annual reviews of network segmentation controls and firewall settings, when applicable, as required by the PCI DSS.

Heads of departments and units: Department and unit heads are responsible for documenting and monitoring departmental procedures, for working with Cybersecurity Operations to ensure proper

technical controls exist, and for ensuring that payment card activities are in compliance. They are responsible for adhering to all PCI DSS requirements and for annually certifying their continued compliance by submitting the appropriate PCI DSS Self-Assessment Questionnaire (SAQ) and supporting university-required documents. Departments/units will be responsible for any fines levied against the university that result from non-compliance. Departments that have merchant IDs owned by George Mason must ensure that applicable SAQs are completed and submitted in a timely manner.

REQUIREMENTS:

Procedures must be documented and be available for periodic review.

Merchant departments seeking approval to accept payment cards must ensure that the following requirements are met:

1. Access to cardholder data (CHD) must be restricted using role-based access controls and network segmentation. User access to cardholder data must be essential to job performance. Each merchant department must maintain a current list of employees who are granted access to CHD and conduct annual justification reviews. All personnel with access to CHD must sign the Payment Card Control and Security Procedures document and must participate in the PCI DSS training annually. Merchant departments are responsible for ensuring that background investigations are performed for applicable personnel per Policy 2221.

2. Cardholder data, whether collected on paper or electronically, must be protected against unauthorized access and systems are hardened to industry standard (e.g., CIS Benchmarks). CHD retention must be based on a documented, legitimate business need and reviewed annually.

3. All equipment used to collect CHD must be protected from tampering and unauthorized use. Devices must be included on the PCI Council's approved PIN Transaction Security (PTS) Device list and authorized by Fiscal Services. Device inspection procedures must be documented and followed.

4. Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment or documents containing CHD. Physical access must be logged and monitored where applicable.

5. Cardholder data (CHD) must not be processed, stored, or transmitted over the University network unless Cybersecurity Operations has approved the configuration and validated all required PCI DSS technical controls. These controls must include network segmentation, strong encryption, properly configured firewalls, and continuous monitoring. In addition, multi-factor authentication (MFA) is required for all remote access to the Cardholder Data Environment (CDE).

6. End-user messaging must never be used to transmit CHD or personal payment information, nor should it be accepted as a method to supply such information. The use of email clients, messaging tools, screen capture utilities, or logging systems to transmit, display, or store cardholder data is strictly prohibited.

7. Transmitting or receiving CHD over voice communication, if necessary, must be done using ITSO-approved methods, such as analog or designated technology explicitly approved for the purpose. Transmission or receiving of CHD over general-use voice communication technology, such as Vonage, is prohibited.

8. Fax transmission of payment card information must only occur on standalone fax machines located in physically secure areas. Multi-function machines are prohibited for the transmission of CHD.

8. Cardholder data must not be retained after authorization unless a legitimate, authorized, and documented business need exists. Any retained CHD must be encrypted and securely stored. Destruction must follow PCI DSS-approved methods. Sensitive authentication data, including the card validation code/value or full magnetic stripe/chip data, must never be stored after authorization, even if this data is encrypted.

9. University staff may not store cardholder data and/or the card validation code/value using any electronic method, including but not limited to storage in databases or spreadsheets or storage on portable electronic media devices.

10. Cardholder data collected on paper must be properly destroyed immediately after processing using approved PCI DSS methods. George Mason has a centralized payment platform that serves as the base for all implementations. TouchNet uCommerce is the University's mandatory payment card system, providing increased control and reduced risk over payment card collection and transaction recording in Banner. Benefits include immediate receipt of the dollars tendered in the sale; amounts are received gross rather than net of fees as required by the Commonwealth Accounting Policies and Procedures (CAPP) Manual; centralized control of reporting for payments; and automatic update of the General Ledger, reducing manual effort. TouchNet is required to notify the University within a specific duration of a security incident and align with the University's Incident Response Plan. Deviations from use of the TouchNet platform require pre-approval, in writing, from the Vice President for Finance or designee. Merchant departments that want to use a third-party service provider other than TouchNet to obtain CHD or be involved with the payment card process must conduct proper due diligence and receive advance approval from the Vice President for Finance or designee and from Cybersecurity Operations.

    Merchant departments are responsible for ensuring compliance with PCI DSS requirements related to third-party service providers, including:

    a. Maintain a written agreement in which the service provider acknowledges their responsibility for the security of CHD they possess, store, process or transmit, or that could impact the security of the CHD environment. All contracts for third party service providers must be authorized by the Vice President for Finance or designee. Merchant departments cannot negotiate their own contracts with payment card processing companies or third-party vendors accepting card payments on their behalf, including acceptance of on-line click-through end user license agreements (EULAs).
    b. Monitor the provider's PCI DSS compliance status annually by either obtaining an attestation of compliance or by verifying the provider is listed on the Visa Global Registry of compliant service providers.
    c. Maintain information about which PCI DSS requirements are managed by the provider and which are managed by George Mason.
    d. Ensure the payment application, when used to process cardholder data, is listed by the PCI Council and/or has been assessed using the Software Security Framework (SSF) by a qualified assessor organization.

11. In the event of an actual or suspected data breach, the incident must be reported to Fiscal Services and Cybersecurity Operations. If fraud is suspected, also contact the University Police.

12. For Departments developing eCommerce applications, architecture and design must be submitted to Fiscal Services and reviewed by Cybersecurity Operations to ensure secure development practices aligned with PCI DSS. The Finance Technology Services (FTS) team will obtain the review on behalf of the department as part of the standard development testing process.

COMPLIANCE:

PCI Compliance is an ongoing process, not a one-time event. The PCI DSS emphasizes "Business as Usual" (BAU) compliant processing and performing continuous compliance activities in an ongoing manner, 24 hours a day, 7 days a week, 365 days a year. Individuals found to have violated this policy, whether intentionally or unintentionally, may be subject to disciplinary action, termination, and could limit an entity's payment card acceptance privileges.

The Vice President for Finance may terminate payment card processing privileges for any entity not in compliance with this standard.

EXCEPTIONS:

All exceptions must be approved by the owner(s) of this standard.

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
Cardholder	The customer to whom a payment card has been issued or the individual authorized to use the card.
Cardholder Data (CHD)	Personally identifiable data about the cardholder gathered as a direct result of a payment card transaction. At a minimum, it consists of the full primary account number (PAN). It may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.
Cardholder Data Environment	Systems and process that store, process, or transmit cardholder data, or can impact the security of cardholder data.
Card-Validation Code/Value	The three-digit or four-digit value printed on the payment card which is used to verify card-not-present transactions. On a MasterCard this is called CVC2. On a Visa card this is called CVV2. On an American Express card this is called CID.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific cryptographic key. Use of encryption protects information from unauthorized disclosure between the encryption process and the decryption process (the inverse of encryption).
Firewall	Hardware and/or software that protect the resources of one network from users from other networks. Typically, an enterprise with an intranet that allows its workers access to the wider Internet must have a firewall to prevent outsiders from accessing its own private data resources.
Magnetic Stripe or Chip Data (Track Data)	Data encoded in the magnetic stripe or chip used for authorization during a card present transaction.

Multi-Factor Authentication (MFA)	Authentication method using two or more distinct forms of verification to prove identity.
Network	A network is defined as two or more computers connected to each other so they can share resources.
PAN	Acronym for “primary account number” and also referred to as “account number.” Unique payment card number that identifies the issuer and the particular cardholder account.
Payment Application	In the context of PCI Software Security Framework (SSF), a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
Role-Based Access Control (RBAC)	A method of restricting access based on a user’s job role, ensuring users can only access data and systems necessary for their responsibilities.
Sensitive Authentication Data	Security data used to authenticate a cardholder and/or authorize payment card transactions. Includes full track data from magnetic stripe or chip, card validation code/value, and PINs/PIN blocks.
Third-Party Service Provider	A business entity that is directly involved in the collecting, processing, storage or transmission of cardholder data on behalf of another entity. This includes companies that provide services that control or could affect the security of cardholder data.

REVIEW SCHEDULE:

This standard, and any related procedures, shall be reviewed and revised, if necessary, annually to become effective at the beginning of the university’s fiscal year, unless otherwise noted.

APPROVAL:

Title, Department Name	Name	Signature and Date
Interim Manager, Cybersecurity Operations	Yu Kuo	Signed by: Yu Kuo F891CB1C79CB4CA... 10/10/2025
Vice President and Treasurer, Treasury Management	Gene Crouch	DocuSigned by: Walter E Crouch 0C98A4B99A7447B... 10/9/2025

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
7/18/2025	1.0	CampusGuard, Fiscal Services (Treasury Management), and Information Technology Services (IT Risk & Compliance and Cybersecurity Operations)	Initial release

RELATED DOCUMENTS/REFERENCES:

- GMU Payment Card Security Policy 2110