THE UNIVERSITY OF RHODE ISLAND

DRAFT

Policy on Payment Card Data Protection

[20261019 DRAFT]

Policy Title	**Policy on Payment Card Data Protection**
Policy #	02.123.1
Policy Owner	Assistant Vice President of Financial Operations and Controller
Contact Information	Questions regarding this policy can be directed to the Director of Treasury at 401-874-4213 or the Chief Information Security Officer at 401-874-4787.
Approved By	President of the University of Rhode Island
Effective Date	_____
Next Review Date	No later than _____
Who Needs to Know About this Policy	All University Units and affiliated organizations, and all employees, contractors, third-party service providers, and other individuals or entities that accept, process, transmit, store, or have access to Payment Card Data on behalf of the University.
Definitions *Defined terms and shorthand references are capitalized throughout.*	**Cardholder Data ("CHD").** Any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder Data includes the primary account number (PAN), which consists of a customer's 16-digit Payment Card number along with any of the following data types: cardholder name, expiration date, and card verification value. **Cardholder Data Environment ("CDE").** The people, processes, and systems that store, process, or transmit Cardholder Data and/or Sensitive Authentication Data. This includes system components that may not store, process or transmit CHD/SAD but have unrestricted connectivity to those components that store, process, or transmit CHD/SAD. **Card Verification Code** (alternatively, "Card Verification Value" or "Card Security Code"). The three- or four-digit value printed on the front or back of a Payment Card. These are also commonly referenced as CAV2, CVC2, CVN2, CVV2, or CID. **Merchant Account.** A financial account established with an acquiring bank that enables an authorized University Merchant to accept, process, and receive settlement of Payment Card transactions. **Payment Card.** Any credit card, debit card, or other card issued by a payment brand (e.g., Visa, Mastercard, American Express, Discover) that is used to make payments. **Payment Card Data.** Any data associated with a payment card that is protected under applicable PCI-DSS including both Cardholder Data (CHD) and Sensitive

DRAFT

	Authentication Data (SAD). This data is classified as Restricted in accordance with the *Policy on IT Data, Systems, and Services*. **Payment Card Industry Data Security Standards ("PCI-DSS").** A set of technical and operational requirements established by the PCI-SSC designed to protect account data and applies to all entities involved in Payment Card processing (including merchants, processors, acquirers, and service providers). **Point of Sale ("POS") System.** Hardware and software used by University Merchants to accept payments from customers, including but not limited to point of interaction devices, PIN pads, electronic cash registers, etc. **Sensitive Authentication Data ("SAD").** Security-related information used to authenticate cardholders and/or authorize Payment Card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks. **Unit.** Any organizational component of the University, including but not limited to its divisions, colleges, schools, departments, offices, centers, institutes, and auxiliary service centers, whether academic, administrative, or otherwise. **University Merchant.** A Unit of the University approved to accept Payment Cards at a given location as payment for goods and/or services or receipt of donations.
Statutes, Regulations, and Policies Governing or Necessitating This Policy	Payment Card Industry Data Security Standard (PCI DSS), Version 4.0.1. PCI Security Standards Council, June 2024 (and any subsequent updates). *Policy on IT Data, Systems, and Services*
Reason for Policy / Purpose	To ensure that all University Units handling Payment Card transactions comply with the Payment Card Industry Data Security Standard (PCI DSS) to protect Cardholder Data, reduce the risk of data breaches, and maintain the University's ability to securely accept Payment Cards.
Forms Related to this Policy	PCI Data Protection Program (Restricted)

Policy Statement

The University of Rhode Island ("University") is committed to protecting Payment Card Data entrusted to the University and maintaining compliance with the Payment Card Industry Data Security Standards (PCI DSS), as established by the Payment Card Industry Security Standards Council.

The purpose of this policy is to establish requirements for safeguarding Payment Card Data received by the University when accepting Payment Cards as a form of payment for goods, services, fees, donations, registrations, or other University-related transactions.

PCI DSS applies to all entities that accept, process, transmit, store, or otherwise handle Payment Card Data. To safeguard the data and reduce the risk of unauthorized access, disclosure, misuse, alteration, or destruction of

such data, the University maintains a Payment Card Industry ("PCI") Data Protection Program ("PCI Program") that establishes administrative, physical, and technical safeguards consistent with applicable PCI DSS requirements. All individuals and entities within the scope of this policy are required to comply with applicable PCI DSS requirements and the University's PCI Program.

I. Scope and Applicability

This policy applies to all University Units and affiliated organizations, and to all employees, contractors, third-party service providers, and other individuals or entities that accept, process, transmit, store, or have access to Payment Card Data on behalf of the University.

The policy applies to all Payment Card activities conducted through University-owned, managed, or contracted systems, services, networks, devices, applications, business processes, and third-party solutions, regardless of whether Payment Card Data is handled electronically, verbally, or in physical form.

II. Roles and Responsibilities

In addition to the standards and responsibilities established in the *Policy on IT Data, Systems, and Services*, the following roles and responsibilities apply to University Cardholder Data Environments:

A. Office of the Controller and the Information Security Office

The Office of the Controller and the Information Security Office ("ISO") are jointly accountable for the development, administration, maintenance, communication, and monitoring of the University's PCI Program.

Responsibilities include:

- Establishing and maintaining PCI Program requirements, standards, procedure templates, and guidance.
- Communicating PCI compliance requirements to University Merchants and other stakeholders.
- Monitoring compliance with the PCI Program and PCI DSS requirements.
- Providing training, awareness, and compliance support to University Merchants and PCI Compliance Leads.
- Conducting or coordinating compliance reviews, risk assessments, and Self-Assessment Questionnaire (SAQ) activities.
- Coordinating the University's response to suspected or confirmed Payment Card security incidents.
- Reviewing and approving Payment Card processing methods, technologies, vendors, and significant changes to existing Cardholder Data Environments.
- Maintaining institutional PCI compliance documentation and reporting requirements.
- Maintaining documented incident response procedures for Payment Card security incidents and conducting periodic tests of such procedures.
- Validating scope and review of Payment Card processes periodically to determine accuracy and completeness of required PCI compliance documentation; advising Unit Leadership on PCI DSS scope reduction methods and opportunities to eliminate unnecessary storage, processing, or transmission of Cardholder Data.
- Requiring corrective action plans and monitoring remediation of identified compliance deficiencies.

In addition, the Office of the Controller is responsible for reviewing and approving the establishment, modification, or closure of all University Merchant Accounts and Payment Card processing arrangements through which Payment Card transactions are settled.

The Office of the Controller and the ISO provide oversight, guidance, and monitoring of the PCI Program; however, responsibility for achieving and maintaining compliance within each Merchant department remains with Unit leadership.

B. Unit Leadership

Unit leadership (e.g. vice presidents, deans, department chairs, directors, and others) with oversight responsibility for a University Merchant are accountable for ensuring compliance with this policy, the PCI Program, PCI DSS requirements, and applicable Payment Card service provider requirements within their areas of responsibility.

Responsibilities include:

- Ensuring that all Payment Card activities within their Units comply with University PCI requirements.
- Establishing, documenting, implementing, and maintaining Unit-level PCI Procedures that align with the PCI Program.
- Ensuring appropriate staffing, resources, and oversight necessary to maintain compliance.
- Designating a PCI Compliance Lead for each University Merchant process.
- Ensuring that employees involved in Payment Card processing complete required training and follow approved procedures.
- Promptly correcting identified compliance deficiencies and implementing required remediation measures.
- Ensuring that only approved payment technologies, systems, vendors, and service providers are used.
- Cooperating with compliance reviews, assessments, audits, and incident response activities.

Units are responsible for any costs, remediation expenses, assessments, vendor fees, technology investments, or other expenditures necessary to achieve and maintain compliance with PCI requirements. In addition, the Units will pay any fees and penalties associated with failure to comply.

C. PCI Compliance Lead

Each University Merchant that processes, transmits, stores, or otherwise handles Payment Card Data must designate a PCI Compliance Lead.

The PCI Compliance Lead serves as the primary departmental liaison to the Office of the Controller and the ISO and is responsible for coordinating PCI compliance activities within the Unit.

Responsibilities include:

- Assisting with the implementation, maintenance, and monitoring of PCI compliance requirements within the Unit.
- Serving as the primary point of contact for PCI-related communications, assessments, audits, and compliance activities.
- Coordinating completion of required PCI compliance documentation, including Self-Assessment Questionnaires and related attestations.
- Communicating PCI requirements, procedural changes, and compliance expectations to personnel involved in Payment Card processing.
- Identifying potential compliance gaps, risks, or control weaknesses and promptly escalating concerns to the Office of the Controller and the ISO.
- Coordinating corrective actions and remediation efforts to address identified deficiencies.
- Ensure completion of the required compliance validation and inventory maintenance practices outlined in Section VII.

- Assisting with incident reporting and response activities involving Payment Card Data or Payment Card systems.

The designation of a PCI Compliance Lead does not transfer accountability for compliance from Unit leadership.

D. Employees Supporting a University Merchant Process

All employees, contractors, and other authorized individuals who participate in Payment Card processing activities are responsible for complying with this Policy, the PCI Program, departmental PCI Procedures, and applicable PCI DSS requirements.

Responsibilities include:

- Completing required PCI security and awareness training.
- Following approved Payment Card handling, processing, and security procedures.
- Protecting Payment Card data from unauthorized access, disclosure, alteration, or destruction.
- Using only approved systems, devices, applications, and processes for Payment Card transactions.
- Promptly reporting suspected or actual security incidents, policy violations, compliance concerns, or unauthorized activities involving Payment Card Data to their supervisor, the PCI Lead for the process they are supporting, the Office of the Controller, or the Information Security Office.

While specific responsibilities may vary by role, all individuals involved in Payment Card processing share responsibility for maintaining the security of Payment Card Eata and supporting the University's PCI compliance efforts.

III. PCI Data Protection Program

The University's PCI Program supports compliance with PCI DSS and the University's obligations to protect Payment Card Data.. The PCI Program establishes the standards, procedures, technical controls, compliance validation activities, and operational requirements necessary to achieve and maintain PCI DSS compliance. It applies to all data, systems, activities, processes, and assets owned, leased, controlled, or used by the University, as well as by its agents, contractors, and other third parties acting on the University's behalf, that are part, connected to, or support a University Cardholder Data Environment. The PCI Program and its associated procedures are integral to protecting the University's financial integrity, safeguarding Payment Card Data, and maintaining confidence in the University's financial stewardship. The PCI Program is designed to:

1. Build and Maintain a Secure Network
   - *Requirement 1*: 1. Install and maintain a firewall configuration to protect Cardholder Data.
   - *Requirement 2*: Do not use vendor-supplied defaults for system passwords and other security parameters.
2. Protect Cardholder Data
   - *Requirement 3:* Protect stored Cardholder Data.
   - *Requirement 4:* Encrypt transmission of Cardholder Data across open, public networks.
3. Maintain a Vulnerability Management Program
   - *Requirement 5:* Protect all systems against malware and regularly update anti-virus software or programs.
   - *Requirement 6:* Develop and maintain secure systems and applications.
4. Implement Strong Access Control Measures
   - *Requirement 7*: Restrict access to Cardholder Data by business need to know.

- *Requirement 8:* Identify and authenticate access to system components.
- *Requirement 9*: Restrict physical access to Cardholder Data.
- *Requirement 10*: Log and monitor access to system components.

5. Regularly Monitor and Test Networks
   - *Requirement 10:* Track and monitor all access to network resources and Cardholder Data.
   - *Requirement 11*: Regularly test security systems and processes.
6. Maintain an Information Security Policy
   - *Requirement 12:* Maintain a policy that addresses information security for all personnel.

The following activities are strictly prohibited:

- Requesting or receiving Payment Card Data through email, fax, chat, text message, social media, or any communication method that has not been approved by the Controller's Office and the ISO.
- Sending, receiving, storing, or temporarily storing Payment Card Data is prohibited unless it is necessary for a legal, regulatory, or business purpose and has been authorized within an approved Cardholder Data Environment.
- Storing sensitive authentication data, including:
  - Card verification codes (CVV/CVC/CID)
  - Full magnetic stripe data
  - PINs or PIN blocks
- Using a personal Merchant Account for university business
- Setting up a University Merchant Account without authorization.
- Processing Payment Card transactions using unauthorized vendors or service providers.
- Connecting unauthorized devices to payment terminals, point of sale devices, systems, or any component of a Cardholder Data Environment.
- Using real Payment Card Data in testing or development environments.

IV. Approval Required Prior to Implementing or Changing Payment Solutions

Units may only use University-approved payment processors, gateways, and point-of-sale systems. Units may accept credit card payments, establish a Merchant Account, implement a payment application, or otherwise process Payment Card transactions only after receiving approval from the Controller's Office and the ISO. Each University Merchant is expected to demonstrate that they have implemented sufficient procedures and established required compliance measures prior to accepting Payment Card transactions and prior to adding, replacing, or upgrading devices; changing any aspect of a Cardholder Data Environment; or modifying Payment Card related procedures.

V. Third-Party Service Provider Requirements

All third-party service providers involved in a University Merchant Payment Card process must be reviewed by the Information Security Office for PCI DSS compliance prior to contract execution and annually thereafter. If a third-party service provider fails to remediate payment card compliance gaps timely, or the deficiency poses a significant risk to the University, the University may suspend Payment Card transaction activity until such time that compliance requirements are met. The University shall maintain a list of third-party service providers, Attestations of Compliance obtained for each, and a documented applicable shared responsibilities chart.

VI. Training Requirements

All University employees involved in processing Payment Card transactions or who have access to a Cardholder Data Environment are required to complete training as part of a security awareness training program prior to accessing or handling Payment Card Data and annually thereafter. The training program, administered by ISO, will be reviewed at least annually and updated to address any new threats and vulnerabilities that may impact the security of a Cardholder Data Environment. The training shall include, but is not limited to, social engineering, phishing awareness, Payment Card Data protection, and incident identification,

VII. Compliance Validation and Inventory Maintenance

University Merchants shall maintain current inventories of payment systems, connected assets, service providers, payment channels, and Payment Card Data flows.

University Merchants shall validate scope and review Payment Card processes periodically to minimize PCI DSS scope and eliminate unnecessary storage, processing, or transmission of Cardholder Data.

Each University Merchant shall complete all required PCI DSS compliance validation activities annually, including completion of applicable Self-Assessment Questionnaires (SAQs), Attestations of Compliance, inventories, and other PCI Program requirements.

VIII. Reporting Violations and Security Incidents

Employees are expected to report any known or suspected Payment Card compliance violations or data privacy and security incidents to the Director of Treasury and the Information Security Office within two hours, or as soon as practicable, of becoming aware of the suspected violation or incident to enable prompt investigation, response, and mitigation.

IX. Enforcement

Violations of this policy will be reported to the Director of Treasury and the ISO. Depending on the nature and severity of the violation, the University Controller may restrict or revoke Payment Card transaction processing capabilities. Additionally, the University may pursue disciplinary action, up to and including termination of employment, as appropriate to the circumstances.

Exceptions

None.

Policy Review and Revisions

(Versions earlier than the first policy number may be paper only)

Policy #	Effective Date	Reason for Change	Changes to Policy
02.123.1	_____	n/a	n/a