Clark University's PCI Compliance Policy

Who Should Read this Policy: All persons who have access to credit card information, including:

- Every employee that accesses, handles or maintains credit card information. Clark University employees include full-, part-time and hourly staff members as well as student workers who access, handle or maintain records.
- Employees who contract with service providers (third party vendors) who process credit card payments on behalf of Clark.
- Employees who manage events and require payment processing capabilities (e.g. Paypal).
- IT staff responsible for scanning the University systems to ensure no credit card numbers are stored electronically.

Name: PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

Purpose: The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

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.

Reason for the Policy: The standards are 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 PCI-DSS requirements as established and revised by the PCI Security Standards Council.

Entities Affected by this Policy:

Tier 1 entities: All departments that collect, maintain or have access to credit card information. These currently include:

- Student Accounts/University Cashier - accept and process credit cards for payment of student accounts
- School of Professional Studies/ALCI - accept credit card for payment of student accounts
- Advancement - accept and process credit cards for donations and alumni events
- IDRISI - accept and process credit cards for purchase of products
- HECCMA - accept and process credit cards for payment of Teaching Certificate Program

Tier 2 entities: All departments managing or sponsoring events that use Paypal or other online payment services approved by the Controller to collect payments through an access point that has been deemed PCI compliant by the University, even though these entities do not have access to credit card information.

Including:

- All departments hosting/sponsoring student activities/programs with payments through Paypal or other online payment service approved by the Controller, (Student leadership & Programming(SL&P), Graduate School of Management (GSOM), IDCE, etc.)
- All academic departments hosting/sponsoring academic conferences/programs with payments through Paypal or other online payment service approved by the Controller.

Tier 3 entities: All departments who have relationships with third party vendors that serve as access points through which Paypal, or any other payment services approved by the Controller, are reached. These departments must confirm PCI compliance on the part of the vendor. Clark’s merchant accounts are not used.

- Athletics - uses IM Leagues for intramural registration

Third Party vendors that process and store credit card information for Clark using Clark's merchant accounts include:
Definitions:

Merchant Account - A relationship set up by the Controller's office between the university and a bank in order to accept credit card transactions. The merchant account is tied to a general ledger account to distribute funds appropriately to the department (owner) for which the account was set up.

Financial Data Manager (FDM) - The Controller of the University who has oversight responsibility for this policy. The Financial Data Manager will also communicate changes to the CIO in order to facilitate enforcement of the policy. The FDM will approve appointment of the Compliance Coordinator and the PCI Department Coordinators.

PCI Compliance Coordinator - The Staff Accountant for Tax and Compliance, who, under the direction of the FDM, will be responsible for staying abreast of changes to PCI DSS requirements, suggesting updates to the policy, coordinating training of Tier 1,2 and 3 entities and serving as point of contact for PCI department coordinators with regard to assessment surveys or other PCI issues.

PCI Department Coordinators - Representatives within Tier 1 departments who are responsible for ensuring that their department has policies and procedures in place to comply with PCI and data security requirements. They will ensure that all departmental personnel with access to credit card data receive appropriate training, read this policy, and sign off on having read this policy. The PCI department coordinator will also be responsible for completing the annual department survey or assessment as required. Appointments of PCI Department Coordinators must be approved by the FDM.

Credit Card Data - Full magnetic stripe or the PAN (Primary Account Number) plus any of the following:
  - Cardholder name
  - Expiration date
  - Service Code

PCI-DSS - Payment Card Industry Data Security Standard

PCI Security Standards Council - The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Self-Assessment - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

Level of Compliance: Credit card companies and financial institutions validate that vendors (Clark) are rated based on their volume of transactions. The rating that a company receives determines the process that they must go through in order to be validated. There are four levels of PCI Compliance, with level 1 being the most stringent and level 4 being the least stringent. If a merchant suffers an attack that has caused account data to be compromised, the merchant level requirement goes up to level 1 automatically. Based on the number of credit card transactions processed annually across the campus (fewer than 20K per year), and the fact that the University has not experienced a breach, Clark would be classified as Level 4. Clark has engaged Security Metrics, a PCI consultant, to assist the university with technical requirements and the completion of our annual self-assessment questionnaire (SAQ).

PCI DSS Version 3.0 Requirements: University policy prohibits the storing of any credit card information in an...
electronic format on any computer, server or database (this includes Excel spreadsheets). It further prohibits the emailing of credit card information. The following list communicates the full scope of the compliance requirements but based on the University policy that prohibits storing of credit card information electronically and Clark’s practice of utilizing third-party vendors for web based credit card processing, some listed requirements may not be relevant.

Procedures:

Clark requires compliance with PCI standards. To achieve compliance, the following requirements must be met:

General Requirements (applies to tier 1,2,and 3 entities):

- Credit card merchant accounts must be approved by the Financial Data Manager
- Management and employees must be familiar with and adhere to the PCI-DSS requirements of the PCI Security Standards Council.
- All employees in Tiers 1,2 and 3 must sign a statement that they have read, understood, and agree to adhere to Information Security policies of Clark University and this policy.
- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by the Financial Data Manager.
- A list of card readers and card processing terminals must be maintained and updated as needed.

Tier 1 Requirements (in addition to the general requirements above):

- Management in departments accepting/processing credit cards must conduct an annual self-assessment against the requirements and submit results to the Compliance Coordinator.
- The PCI Department Coordinator must create or confirm the existence of appropriate policies and procedures for credit card processes, storage, and destruction of card data.
- Job descriptions for employees with access to credit card data must be reflective of this access and must include data security requirements associated with access.
New employees must undergo PCI training upon hiring.
Existing employees must undergo PCI training annually.
Access to the cardholder data environment must be restricted to only those employees with a need to access and physical controls must be in place to protect the cardholder data environment.
Terminals/readers must be routinely examined for evidence of tampering and any evidence brought to the attention of the Compliance Coordinator.

Tier 2 Requirements (in addition to the general requirements above):

- Management in Tier 2 departments using Paypal or other Controller approved online payment services for event payments must ensure that all personnel within their department understand that Clark prohibits anyone from accepting credit card information or processing credit card payments on behalf of the “customer”.
- Employees managing/sponsoring events for which Paypal or other Controller approved online payment services are used must confirm knowledge of and adherence to the above policy when requesting Paypal or other approved online payment service access/mailbox from the Financial Data Manager.

Tier 3 Requirements (in addition to general requirements above):

- Management in Tier 3 departments must confirm that the third party vendors through whom they are accessing Paypal or other Controller approved online payment services are PCI compliant.

Storage and Disposal

- Credit card information must not be entered/stored on any electronic device—this includes University network servers, workstations, laptops, tablets and cell phones—unless it is explicitly approved for use as part of the cardholder data environment.
- Credit card information must not be transmitted via email
- Web payments must be processed using a PCI-compliant service provider approved by the Financial Data Manager on only computers designated by ITS as belonging to the secure cardholder data environment. Credit card numbers must NOT be entered into a web page of a server hosted on the Clark network.
- Although electronic storage of credit card data is prohibited by this policy, the University will perform a quarterly network scan against the cardholder data environment to ensure that the policy has not been violated.
- Any paper documents containing credit card information should be limited to information required to transact business, those individuals who have a business need to have access, should be in a secure location, and must be destroyed via cross-cut shredding or placement in a secure shred bin 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.
- Sensitive cardholder data must be destroyed 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 cross-cut shredding in house or with a third-party provider with certificate of disposal.
- Neither the full contents of any track of the magnetic stripe nor the three-digit card validation code may be stored in a database, log file, electronic document or point of sale product.

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

- The Financial Data Manager must approve each merchant bank or processing contract of any third-party vendor that is engaged in, or proposes to engage in, the processing or storage of transaction data on behalf of Clarkregardless of the manner or duration of such activities.
- The Financial Data Manager must ensure that all third-party vendors adhere to all rules and regulations governing cardholder information security.
- The Financial Data Manager must 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.
- Information must be maintained about which PCI-DSS requirements are managed by each third party provider and which are managed by Clark.
Additional Requirements:

- Complete an annual self-assessment—both at the Tier 1 entity and University level
- Perform a quarterly network scan

Without adherence to the PCI-DSS standards, the University would be in a position of unnecessary reputational risk and financial liability. Merchant account holders who fail to comply are subject to:

- Any fines imposed by the payment card industry
- Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees
- Suspension of the merchant account

Self-Assessment

- The PCI Compliance Coordinator will notify each Tier 1 entity ahead of the time-line to complete and submit the annual departmental assessment. This assessment is the responsibility of the PCI Department Coordinator.
- The PCI-DSS Self-Assessment Questionnaire must be completed at the University level by the merchant account owner annually and anytime a credit card related system or process changes.

Training

- Annual employee training programs must be offered to train employees on PCI DSS and the importance of compliance. This will be made available by the Financial Data Manager and coordinated by the PCI Compliance Coordinator. PCI Department Coordinators must ensure that employees with access to card data within their departments take part in annual PCI training and that all new employees within these departments take part in PCI training upon hiring.

Responsible Organization/Party: The Controller shall serve as the Financial Data Manager of the policy which includes responsibility for notifying the Information Security Officer, applicable Department Heads and Data Managers about changes to the policy. S/he will be assisted by the CIO, the Staff Accountant for Tax and Compliance and University Officers as needed.

Enforcement: The Information Security Officer will oversee enforcement of the policy. Additionally this individual will investigate any reported violations of this policy, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the policy. S/he will be assisted by the CIO, Controller, and the Staff Accountant for Tax and Compliance as well as other University Officers as needed.

Additional Resources

PCI DSS Requirements and Security Assessment Procedures: