PRINCETON DEPARTMENTAL PCI ATTESTATION OF COMPLIANCE

March 2017

Every department at Princeton University that accepts credit or debit cards as a form of payment handles confidential information including but not limited to credit/debit card numbers, expiration date, and CVV codes. The improper handling of this information could subject the University to fines, increased credit or debit card transaction fees and/or the suspension of our credit or debit card privileges.

The Payment Card Industry requires that this cardholder data is handled, transmitted, and stored according to Payment Card Industry Data Security Standard (PCI-DSS), so that it is not easily stolen and misused. Princeton University is committed to handling cardholder data in accordance with PCI-DSS, and therefore requires the following of each Department that accepts credit cards as a form of payment:

- Access to applications with cardholder data is limited to authorized individuals whose jobs require such access. User privileges are based on job function, and access rights are restricted to the least privileges necessary to perform job responsibilities.
    - Applications processing credit card transactions are configured so that only a System Administrator can add users to the system.
    - Only individuals authorized by the Academic or Administrative Manager are added to the application by the System Administrator
    - Each authorized User has a unique account and password, and does not share their account and password with anyone.
    - A background check has been conducted on any new hire that handles cardholder data
    - In instances where a single administrative account must be shared amongst authorized application admins (e.g. some sort of limitation of the application itself), a second unique form of authentication (identification) must be used (e.g. Secure token) in order to gain access to the application
    - Access to and querying of the cardholder database is restricted to the database administrator
    - Access to systems with cardholder data is revoked immediately if a user is terminated
    - A list of authorized individuals and their job title has been provided to Cash Management.

- Authorized Users within the Department that accept, capture, store, transmit and/or process credit or debit card transactions have been authorized, and have successfully completed the required University's PCI Compliance Training Program. Academic and Administrative Department Managers, Deans, and Directors maintain a record of individuals who have completed training in their areas.

- All individuals in the Department handling cardholder data have read the requirements stated in the University's **Credit Card Processing Policy for Merchant Locations** ("Policy"), and accept process, handle and store cardholder data in accordance with the Procedures set forth by this Policy.

- Individuals in the Department with access to cardholder data protect the information in the manner specified within the Policy:

    - Effectively protect the credentials (IDs and passwords) and the computers or terminals that they may use to process credit or debit card transactions
    - Keep terminals in a secure location and inspect them periodically for tampering or substitution
    - "Media" including but not limited to computers, removable electronic media, paper receipts, paper reports, faxes, and answering machines that contain cardholder data is locked up in an area where access is strictly controlled, and limited to authorized individuals. Media containing cardholder data is never moved out of a secure area or

distributed without prior approval from Cash Management, and the use of secure delivery methods that log and track the Media.
    - Destroy credit or debit card information as soon as it is no longer required, using methods prescribed in the Policy.
    - Never transmit cardholder data via end user messaging, including e-mail, instant messaging, or chat, and tell customers that the University does not accept credit card information that is sent to us via e-mail, instant message or chat.
    - Use only University owned "DeSC Standard" computers that are managed centrally by OIT, or **Approved Terminals and Devices**, sourced from designated vendors to capture or process credit or debit card transactions, or has met with OIT and obtained approval to use an alternate computer or device.
    - When remotely accessing cardholder data, never copy or move cardholder data onto a local hard drive or removable drive.

- If the Department has a website/webserver that accepts online payment by credit or debit card and redirects users to a secure payment gateway:
    - The website must be reviewed and approved by Cash Management and OIT
    - First Data Global Gateway should be used to capture and transmit cardholder data to the University's payment processor. Alternative secure gateways are only permitted if they have been approved by Cash Management.
    - The webserver must be located in a secure environment approved by OIT, located outside of the University's PCI Compliant Computing environment
    - Appropriate software development practices need to be followed for the creation and maintenance of any web site or applications that store, process, or transmit cardholder data or that can impact the security of the Cardholder Data Environment. Prior to development, the department will contact Cash Management for a list of current practices and/or to discuss options

- If the Department uses third party applications software that accepts payment by credit card
    - Service providers must acknowledge that they are responsible for the security of cardholder data they possess or otherwise store, process or transmit on behalf of Princeton University.
    - Service Provider contracts must be reviewed and approved by Cash Management for PCI language and Confidentiality provisions.
    - Service Provider contracts, and contract renewals executed by the department must be submitted to Cash Management.
    - The Department must conduct required due diligence on the software application in conjunction with Cash Management, to ensure that the application is properly configured, and to determine how cardholder data is captured, transmitted and stored by the application.
    - If the application software is not compatible with First Data Global Gateway, another Secure Gateway may be used, but must be reviewed and approved by Cash Management.
    - Each year the Department must verify with Cash Management that any third party software applications being used by the Department, which handle cardholder data, are PCI compliant and is in compliance with PCI PA-DSS.

- Except on computers/terminals/registers used only for cashiering at a point of sale, the Application must be configured to meet all PCI requirements for User IDs and passwords which are not satisfied by the University's general network:
    - Disable inactive user accounts within 90 days.
    - Lock out user ID's after no more than six failed attempts, with lockout duration set to a minimum of 30 minutes or until an administrator enables the User ID

- Require users to change their passwords at least every 90 days and submit a new password that is different from any of the last four passwords he or she has used.
- Require strong passwords with minimum length of at least 7 characters that contain both numeric and alphabetic characters
- Verify user identity before permitting modification to any authentication credential, such as a password reset or provisioning of new token
- Require users to re-authenticate or re-activate the session after being idle for more than 15 minutes.
- Login via remote access to applications handling cardholder data requires the use of multi-factor authentication.

- If a breach of credit or debit card information is suspected or has occurred, the Department Manager will immediately report the breach to the OIT Help Desk at 258-HELP.

- If the Department has an Application which stores cardholder data in the University's PCI Computing Environment, the department has conducted a due diligence call on the Application software with Cash Management, OIT and the vendor, and has documented and implemented procedures established by OIT for their Merchant Location and software application.

To the best of my knowledge, the Department for which I am responsible is PCI compliant and adheres to the above University requirements, and the attached list of authorized individuals, third party applications software, and computers/terminals used to process credit and debit cards is complete and accurate.

Department: _____

Department Manager, Dean or Director: _____

Signature: _____

Individuals authorized to accept and process credit or debit cards and other individuals who have access to cardholder data

Name	PU Net ID	Role	Administrator Privileges (Yes/No)

University Asset Tag #/ serial # of computers (including web servers) and terminals that capture cardholder data or process credit or debit card transactions

Make/Model	Business Function for Device	Location	Serial #/ Asset Tag

PU Websites and Third Party Software Applications used to process credit or debit card transactions

PU Website / Secure Gateway / Third Party Service Provider	URL (if applicable)	Description of Website, Service, Secure Gateway, or Application