Credit Card Processing and Handling Policy

This policy was approved by the President's Cabinet on April 21, 2015.

PROFILE

To protect the credit card data of our students, faculty, staff, donors, and guests - as well as to comply with the Payment Card Industry Data Security Standards (PCI-DSS), the State University of New York at New Paltz must set standards and procedures for secure and reliable processing of credit card data.

SCOPE

This policy applies to all employees of the State University of New York at New Paltz who have access to credit or debit card numbers accepted for payments to the College.

DEFINITIONS

- Cardholder Data - The full magnetic stripe data of the card, any portion of the card number beyond the last four digits and card expiration date.
- 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 Card Verification Codes (CVV, CVC, CSC, etc.)
- PCI-DSS - The Payment Card Industry Data Security Standard - an information security standard for organizations handling credit cards from the major brands.
- Cardholder Data Environment - Systems which are involved in the processing or transmission of cardholder data, along with those systems deemed to be involved with those credit card data, or with access to systems involved with credit card data.
- P2PE - Point to Point Encryption. This refers to credit card processing terminals

POLICY

Departmental Acceptance of Credit Card Payments

- A department can only accept credit cards with the explicit written approval of the Vice President of Finance & Administration, or the Assistant Vice President of Finance & Administration.
- For security purposes, technology purchases must be reviewed and approved by the Chief Information Officer, or the Information Security Officer.
- Service contracts with vendors or payment processors must be reviewed and approved by the Vice President of Finance & Administration, or the Assistant Vice President of Finance & Administration.

Access to Customer Credit Card Data

- Access is authorized only for College personnel who are responsible for processing or facilitating credit card transactions. Such authorization must be granted by the Vice President of Finance and Administration, or their designees.
- Departments who have been approved for access must keep (and provide to the Internal Controls Coordinator) a list of staff who are involved in credit card processing. This list must be updated within a week of personnel changes.
- Such access can only occur in specific locations approved by the Vice President of Finance and Administration, the Assistant Vice President of Finance & Administration, or their designees. A special exception may be granted for mobile card processing systems.
- Only authorized College personnel may process credit card transactions or have access to documentation related to credit card transactions.
- A copy of this policy must be read and signed by authorized personnel upon initial employment and annually thereafter.
- Signed policies will be maintained by the department supervisor.
- All electronic systems in the Cardholder Data Environment must require authentication. Such authentication must provide an account per user, and should not have group accounts for more than one individual.
- Access to systems in the Cardholder Data Environment for vendors and business partners will be granted only if absolutely necessary. Such access will be immediately disabled after the need for such access passes.

Transmission of Credit Card Information

- Insecure transmission of cardholder data is prohibited. Cardholder data can only be transmitted via approved encryption protocols and methods, which may change over time due to newly discovered security vulnerabilities.

Receipt of Credit Card Information via Email

- Under no circumstances should cardholder data be sent or requested via email.
- A standard template advising the sender that the transaction cannot be processed should be sent in reply (with the credit card information in the original email redacted). The email should offer acceptable methods for making payments through the departments existing approved procedures.
- The message containing the cardholder data should then be immediately deleted (and deleted from the trash).

Telephone Payments

- When recording credit card information for processing, only cardholder name, account number, expiration date, zip code, and street address may be recorded. It is not permissible to record and store the sensitive authentication data (including the three digit security code.
- Such a code can be asked for over the phone if it will be entered into a secure, approved Point-to-Point Encrypted terminal.
- If cardholder data needs to be kept before processing, it should be stored in a secured (locked) area before processing.

Processing Credit Card Transactions on Campus Computing Devices

- Offices that make payment card transactions on a computer (by entering a customer's credit card number on a website or through a vendor's payment software) must do so from a computer or device designated and approved for that purpose.
- These computers must be setup and secured by the Faculty/Staff Help Desk as per internal Computer Services procedures, and placed on the restricted PCI VLAN (Virtual Local Access Network).
- Card numbers must never be entered on any computer or device not on the PCI VLAN.
- The credit card may only be swiped (or have its internal chip read) by systems on the PCI VLAN, or using an approved P2PE card reader.

Storage of Credit Card Information

- Electronic storage of cardholder data, or sensitive authentication is **expressly prohibited under any circumstance**.
- Cardholder data should be retained in a secure location only as long as is necessary for business purposes. Cardholder data must be destroyed when no longer needed (via cross-cut paper shredders, or by being placed in a shred box provided by Internal Controls).
- Sensitive authentication data must be immediately destroyed after the transaction is processed.

Equipment Verification & Storage

- Credit card processing equipment should be inspected and verified to detect any tampering. The procedure for such verification and the frequency of inspection will be determined by the Internal Controls Coordinator.
- Mobile credit card processing equipment (any equipment not used exclusively at a specific desk), including any readers attached to laptop computers, smart phones, or tablets, should be kept in a secure location when not in use. Standards for securing this equipment will be set by Internal Controls and may differ depending on the usage and location of the devices.

Additional Policies & Documents

This policy supplements the following campus policies (as well as any department specific policies);

Acceptable Uses and Privacy Policy

Information Security Policy (*pending)*

Confidential Information Policy

Incident Response Policy