PennState
New Kensington

Credit Card Use Procedure

Procedure Number: PSU-NK-ITS-002
Date: February 15, 2018
Page Count: 4

Purpose:

Establish operational conditions and guidelines for the use of credit card data in line with University policy, Payment Card Industry (PCI), Data Security Standards (DSS) and state and federal regulations.

Scope:

This procedure represents and provides the minimum security requirements, appropriate guidelines, and business practices required to protect the confidentiality, authenticity, and integrity of credit card payment information against unauthorized or improper use. This procedure establishes the minimum operational standards required to offer credit card payment options to University customers and governs all University owned and managed properties, equipment, and employees or agents representing the University. Administration of this procedure is handled by the Business & Finance department but since it addresses electronic transmission and storage of credit card data, the procedure is classified as an Information Technology procedure.

Definitions:

Access and Security Representative (ASR) – the individual that enforces all University policies and guidelines pertinent to the use of University computerized data assets. He/she acts as liaison between a specific work unit and the AIS Security Office. Whenever problems, questions, or issues must be brought to the attention of the Administrative Information Services (AIS) Security Office, the ASR becomes involved. The ASR would also become involved during investigations of security violations and other security issues. The campus ASR is Jason Bush.

Credit Card Data – A cardholder's Primary Account Number (PAN), name, service code, and expiration date. This also includes sensitive authentication data, including the contents of the credit card magnetic stripe, CVC2/CVV2/CID number, and PIN / PIN Block

Credit Card Data Steward (Data Steward) – A University employee responsible for the use, storage, and processing of credit card data.

Merchant – A business or entity accepting credit cards as a method of payment for goods or services.

Procedure:

Physical Security

User Access

- Credit card data should be accessed by essential employees only and identified as credit card data stewards. The department director or budget administrator is responsible for:
    - Identifying essential staff member(s) (data stewards) who will use, store, and process credit card information.
    - Alerting the campus Access and Security Representative (ASR) when the data stewardship responsibility of the use, storage, and processing of credit card information has changed or is initiated.
- Access to credit card data by outside agencies, contractors, or consultants is prohibited.
- University employees defined as data stewards must acknowledge in writing that they have read and understood the contents of this procedure.
    - The campus ASR is responsible for ascertaining and storing a signed written acknowledgement from each campus data steward.

Physical Access

Classification of Data

- Credit card data must be classified as "confidential" and when stored must be placed in a folder clearly marked with a data classification cover sheet identifying the institution, data steward, contact information (name, telephone number, and email address) and classification type (confidential).

Physical Storage

- When credit card data is not being processed or destroyed by a data steward, it must be stored in a locked physical enclosure in which the data steward is the sole individual with access to the enclosure.
- The acceptance, storage, and processing of credit card data is restricted to property owned and/or managed by the University.

Distribution of Credit Card Data

- Relocation of credit card data to a new physical location is prohibited unless a written exception is granted by the Chancellor and campus ASR.
    - Credit card data, if distributed, must be classified as confidential and sent via secure courier or other delivery method that can be accurately tracked.

Credit Card Data Destruction

  - Once credit card data is processed it must be destroyed. Paper documents containing credit card data must be incinerated, cross-cut shred, or pulped. If paper documentation is incinerated, a certificate of destruction is required and must be submitted to the campus ASR upon destruction.
    - Transactional data, such as the cardholder's name, address, charged amount, card type, and transaction number must be archived for seven years per the University financial retention schedule. Only credit card data, as defined above, must be destroyed.

Electronic Access & Security

- Credit card swipe terminals approved by the University Controller's office is the only acceptable method for processing credit card data.
- Electronic storage or transmission of credit card data is strictly prohibited.
  - Storage of credit card data on a computer, external storage device, and electronic media
  - Use of email or electronic messaging to accept, store, or transmit credit card data is prohibited.

Acceptable Use

- Fax, mail, and/or telephone are satisfactory methods of accepting credit card data from a customer.
  - Upon receipt, credit card data must be given to the appropriate data steward to store, process, and destroy.
  - Accepting credit card data via email or other electronic medium is strictly prohibited.

Breach of Credit Card Data

- If a data steward suspects the unauthorized or improper use or breach of credit card data, he or she must immediately report such situations to the Office of Information Security (OIS) and the campus ASR. If an information technology resource was involved during the breach, the Director of Information Technology must also be notified.
  - The Office of Information Security (OIS), in coordination with appropriate University offices, will determine if financial loss has occurred and if control or procedures require modification. When warranted by such preliminary review, University Police Services, Internal Audit, and other University departments or law enforcement authorities will be contacted as appropriate.

Procedure Review, Change Notification, and Training

- The campus ASR is required to review and update this procedure annually to assure compliance with current Payment Card Industry Data Security Standards (PCI-DSS).

  - If/when the procedure is updated, the campus ASR is required to send notification to the campus Chancellor, departmental directors, and data stewards affected by or as defined and identified by this procedure.
- Data stewards are required to attend an annual security awareness training program offered by the University Information Privacy and Security (IPAS) group.

Audit

- The campus ASR is responsible for periodically auditing campus data stewards to ensure procedure compliance.

Procedure History:

February 15, 2018 – Procedure created based off previous campus policy.