# Payment Card Industry (PCI) Compliance Policy

**Date**
10/23
**Policy Scope**

The University of Southern Indiana is committed to compliance with the Payment Card Industry Data Security Standards (PCI DSS) to protect payment card data regardless of where that data is processed or stored. All members of the university community must adhere to these standards to protect our customers and maintain the ability to process payments using payment cards.

The university prohibits the retention of complete payment card primary account numbers (PAN) or sensitive authentication data in any university system, database, network, computer, tablet, cell phone, or paper file.

**PCI Background**

The PCI DSS is a mandated set of requirements agreed upon by the major credit card companies. The security requirements apply to all transactions surrounding the payment card industry and the merchants or organizations that accept these cards as a form of payment.

The university must comply with the PCI DSS in order to accept card payments and avoid penalties. This policy and additional supporting policies:

- Provide the requirements for processing, transmission, storage, and disposal of cardholder data transactions
- Reduce the institutional risk associated with the administration of payment cards
- Promote proper internal control
- Promote compliance with the PCI DSS

**Roles and Responsibilities**

This policy applies to those involved with payment card handling including employees, contractors, third-party vendors, individuals, systems, networks, and other parties with a relationship to the university including any unit using third-party software to process payment card transactions. This includes transmission, storage, and processing of payment card data, in any form (electronic or paper).

**All Users**

- Safeguard cardholder data.
- Report occurrences of possible incidents and data breaches to the Information Security Officer.
- Review and comply with the following university policies:
    - Information Security Policy
    - Data Communication and Computer Use Policy

**IT Security Committee**

- Monitor the university's compliance with PCI DSS requirements.
- Review and coordinate the completion of the required annual SAQ self-assessment.
- Assist with mandatory annual training sessions.
- Collect departmental PCI procedures as part of the annual SAQs.

**Information Technology**

- Maintain security standards required by PCI DSS.
- Keep current with PCI DSS regulations and make changes to systems and processes, as appropriate.

**Business Office**

- Maintain an inventory of all areas that process payment card transactions using an approved merchant account, or other compliant methods.
- Maintain the inventory of all devices, merchant ids, and terminal ids along with activation status.
- Administer user access add and remove activities, including conducting annual user review of credit card provider access.
- Assist with mandatory annual training sessions.
- Assist with completion of the annual self-assessment documents (SAQs).
- Evaluate compliance with PCI as part of scheduled cash handling reviews.

**Departments (who accept payments)**

- Review and comply with the following Business Office procedures:

**"University Money Handling Procedure"**

- Maintain departmental Standard Operating Procedures (SOP) for PCI compliance and verify staff has an understanding of the procedures and their responsibilities.

Policy Standards

**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 Business Office and coordinated by the IT Security Committee. Department supervisors 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.

**Transmission**

- All payment card transmission will utilize fully encrypted pathways from the card entry to the payment processing merchant.

**Security Incident and Identification**

- Employees must be aware of their responsibilities in detecting security incidents. All employees have a responsibility to assist in the incident response within their departments. See IT Security Information Security Policy for more details.

**Data Retention and Disposal**

Do not store cardholder data unless it is absolutely necessary.

- If it is necessary to retain cardholder data, make every effort to keep cardholder data to a minimum, and destroy when no longer needed.
- Data retention and disposal procedures should limit the storage of cardholder data to that which is required for business, legal, and/or regulatory purposes.
    - For electronic cardholder data records:
        - Destroy (shred, crush, overwrite, or degauss) any computer media (hard drives, portable storage) that contained cardholder data when those devices are retired, or the data are no longer needed.
        - Redact imaged documents to remove cardholder data information.
    - For paper-based cardholder data records:
        - Cross-cut shred, incinerate, or pulp paper documents containing cardholder data when no longer needed.

- Do not store sensitive authentication data in any form after authorization, even if the data is encrypted. Sensitive authentication data includes:
  - Primary credit card account number
  - Full contents of the magnetic stripe
  - Card Verification Code or Card Verification Value (CVC/CVC2/CVV/CVV2/CID)
  - Personal Identification Number (PIN) or the encrypted PIN block

**Revision History**

| Revision # | Description | Approval | Date |
|---|---|---|---|
| **1.0** | New policy | S. Draper- Author;<br>IT Security Team, Business Office, and S. Bridges- | 7/31/2022 |