

PCI Compliance Procedures and Guidelines

All University departments and affiliated units wishing to accept credit cards must comply with [University policy](#), including the Payment Card Industry Data Security Standards.

Arrangements to accept credit and/or debit cards payments must be approved through the Comptroller's Office. This document details procedures to implement credit services at Illinois State University. Contact David Carson at 438-8076 for more information.

The Comptroller's Office will assist departments engaged in credit card sales in the proper procedures for processing credit card transactions. Selling departments will be assessed the bank service fee on all credit card sales transactions. Departments are responsible for Illinois Sales Tax if applicable. Questions on the applicability of Sales Taxes, and related reporting requirements should be addressed in the E-Commerce Business plan application.

There are three components to the management of sales transactions.

1. **Storefront.** The term refers to the mechanism for acquiring the goods or services. This may be as simple as a posted pdf form for surface delivery, or as complicated as a shopping cart. This refers to the customer portion of the transaction.
2. **Payment.** This term refers to the collection, transmission and authorization of the credit or dollar amount for the transaction.
3. **Business process.** This term refers to the management and operational elements involved in the transaction including staff, accounting practices, training elements, and physical environment.

I. Approved Options:

- A. **Web storefront to Touchnet Gateway:** A web site storefront to display products and services developed by the selling department, assisted by Institutional Web Support or Administrative information Systems, an electronic link to the TouchNet gateway software and an approved network connection provided by Telecommunications and Networking. This is the preferred methodology for all Illinois State University transactions involving the acceptance of payments by credit card via the Internet.
- B. **Accepting credit card numbers via fax, phone or hardcopy forms:** Departments may either use a card present device and hand enter the credit card number or use a stand-alone personal computer used for the sole purpose of entering credit card numbers into the department's secure website. Methods for securing and providing for the safety and the retention of personal and financial information on written records would apply.
- C. **Third party software storefront and web payment:** Selling departments will contract through the Comptroller's Office for all third party payment solutions. A vendor PCI compliance statement is required for all third party payment solutions.

- D. Card Present: Approved card present devices will be purchased through the Comptroller's Office and deployed with the assistance of Telecommunications and Networking.

II. Unacceptable Options

- A. E-Mail Transactions: E-mail must not be used to transfer confidential data/information such as credit card number, social security number, purchaser identification, or other sensitive information related to the purchaser.
- B. Unsecured Fax.
- C. Campus Mail (unsealed). Credit transactions must be sent in a sealed, standard envelope. Campus Mail envelopes are not acceptable.

III. Business Plan Review and Approval Process for Proposed E-commerce Applications:

- A. Prior to development of an e-commerce application, including those developed by or acquired through outside contractors, the selling department must submit a business plan to initiate review. Applications for business plan review must be submitted to the E-Commerce Committee at Campus Box 1200.
 - 1. Describe the products or services to be offered and the rationale for offering them via e-commerce.
 - 2. Provide estimated annual transaction and dollar volume.
 - 3. Describe the business process to handle the additional workload from the e-commerce function, including the accounting, maintenance, and reconciliation of general ledger accounts and the credit card operation.
 - 4. Indicate whether the operation currently accepts credit cards.
 - 5. Identify the hardware requirements and hardware location.
 - 6. Identify the source of technical support.
 - 7. Identify areas or departments that need to be involved in the development and implementation of your e-commerce initiative; examples may include Finance, Information Systems and Technology, or Procurement and Contract Services.
 - 8. Identify the working group to develop the initiative.

The Comptroller's Office will:

- 1. Administer the process of obtaining new merchant numbers
- 2. Conduct annual reviews of existing merchants regarding safeguarding and storage of cardholder information. (Credit card handling procedures are always subject to audit by internal and external auditors or charge card review firms.)

3. Provide annual training on the secure storage and disposal of all non-ecommerce credit card paper transaction records in conjunction with cash handling training.
4. Provide guidance on completion of Self-Assessment Questionnaires.

Administrative Information Systems will:

1. Review and approve implementation of any technology changes and payment gateways associated with credit card transactions processing.
2. Conduct periodic assessments of security controls in place to protect PCI related technology implementations, including but not limited to periodic network-based vulnerability scans.
3. Provide guidance on completion of Self-Assessment Questionnaires.

Telecommunications and Networking will:

1. Prepare protected network segments to properly isolate commerce transactions
2. Provide and review pertinent network logs
3. Provide guidance on completion of Self-Assessment Questionnaires

B. Annual Review and Training

1. Each department conducting E-commerce must complete an annual review initiated by the Comptroller's Office. The review will certify that the department is conducting E-Commerce in the manner approved by the E-commerce Committee and adhering to university policies. Any significant changes to E-commerce business activities or departmental contacts should be noted.
2. Annual Training will be conducted in accordance with PCI requirements.

C. Enforcement

1. E-commerce processes not in compliance with University policy will be removed from service. Staff who manage non-compliant E-commerce processes, their supervisors, and unit administrators may be subject to penalties and disciplinary action, both within and outside the University. Violations will be handled through the University disciplinary procedures applicable to the relevant unit or employee.

D. Remediation (existing processes). In order for the University to achieve compliance with the credit industry, all processes are subject to validation. Existing services will be reviewed under the Business Plan guidelines and receive approval by July 30, 2007 or be subject to the enforcement in section III-C, and other pertinent policies and applicable laws and regulations.