

# Minimum Security Standards for Merchant Payment Card Processing

---

1. Purpose .....	1
2. Scope .....	1
3. Standards .....	2
4. Additional Resources .....	3
5. Revision History .....	3
6. Approvals .....	4

## 1. Purpose

U. T. Austin is committed to maintaining the security of customer information, including payment cardholder information such as payment card account number, payment cardholder name, expiration date, and payment cardholder verification number. To uphold this commitment, U. T. Austin follows the best practices for protecting payment card information as defined by the [Payment Card Industry Security Standards Council](#), including information in computer systems which process, store, and transmit payment card information. U. T. Austin must adhere to these standards to limit its liability and to continue to process payments using payment cards. Scope

## 2. Scope

[The PCI Data Security Standard](#) impacts all U. T. Austin computers and electronic devices involved in processing payment card information. PCI compliance is required of all eCommerce merchants that store, process or transmit credit cards, use equipment with external facing IP addresses, and all other payment channels including manual processing techniques such as, but not limited to, point-of-sale terminals and cash registers.

U. T. Austin, including all colleges, schools, and units that process payment card data, has a contractual obligation to adhere to the PCI Data Security Standard (PCI-DSS). The Controller's Office and the Information Security Office are working with departments to assure compliance by December 31, 2007

### 3. Standards

To meet the Payment Card Industry requirements, the Information Security Office requires the following actions be taken:

1. All Merchant accounts must be obtained through and registered with U. T. Austin [Cash Management Services](#).
2. All Merchants must utilize the U. T. Austin central processing services, [What I Owe](#) and/or [TXShop](#), for their payment card processing needs, unless the university Executive Compliance Committee (or its designate) has approved an [exception](#). When an exception has been granted, the university merchant remains responsible for ensuring the vendor providing payment card processing services is PCI compliant. The university merchant will coordinate proof of compliance with U. T. Austin Cash Management Services.
3. If utilizing the central processing services, merchants shall not transmit or store cardholder data outside the centralized system.
4. All systems processing payment card information must be registered with the UTnet Utilities (your local Technical Support Coordinator(s) 'TSC' can assist you). An appropriate description for these devices must be provided in the description field and the priority should be set as 'Critical'. The merchant manager should be included as an additional Security Custodian.
5. All systems processing payment card information must comply with the Category-I requirements specified in the U. T. Austin [Minimum Security Standards for Systems](#). Server administrators should also refer to the [Server Hardening Checklists](#).
6. All applications processing payment card information must comply with the U. T. Austin [Minimum Security Standards for Application Development and Administration](#).
7. All payment card business and data handling processes must comply with the U. T. Austin [Minimum Security Standards for Data Stewardship](#).
8. All eCommerce merchants processing less than 20,000 payment card transactions per year, and all non-eCommerce merchants, are considered **Level-4 Merchants** by PCI Standards. UT Austin Cash Management will determine PCI Level. All eCommerce systems associated with the **Level-4 Merchant's** processes shall undergo quarterly vulnerability scans, which will be conducted by the Information Security Office. Local Technical Support Coordinators (TSCs) are expected to review the vulnerability scan results and remediate or take steps to mitigate the risk. The TSCs will note in the Information Security Office's vulnerability management console if a particular vulnerability is identified as a false positive or the risk has been mitigated in other ways.
9. All eCommerce merchants processing 20,000 to 150,000 payment card transactions per year per card type are considered **Level-3 Merchants** by PCI Standards. If Visa transactions are less than 20,000 and MasterCard transactions are less than 20,000 then merchant is still considered Level 4. However, separate merchants processing under the same infrastructure will be combined to determine PCI Level. UT Austin Cash Management will determine PCI Level. All systems associated the **Level-3 Merchant's** processes shall undergo periodic vulnerability scans by the Information Security Office. Additionally, all systems associated with the **Level-3 Merchant's** processes shall undergo at least quarterly vulnerability scans conducted by an approved PCI vendor. The **Level-3 Merchant** shall be responsible for paying for these services and will

coordinate all activities with U. T. Austin Cash Management Services and the Information Security Office.

10. All **Level-3 and Level-4 Merchants** shall annually complete a PCI Self-Assessment Questionnaire via the Information Security Office’s risk assessment application, [ISORA](#). Access to these surveys will be limited to the respective department’s Technical Support Coordinator(s), the department contact(s) for the merchant account, and the department head. All responses shall be coordinated with U. T. Austin Cash Management Services and the Information Security Office.
11. All systems processing payment card information must use fixed IP addresses. Access to these systems should be appropriately restricted.
12. Using any wireless connectivity for payment card processing is not authorized unless purchased from Global Payments Inc through UT Austin Cash Management. Merchants that must use wireless must file an exception via the U. T. Austin [Exception Reporting Process](#) and must adhere to PCI best practices regarding such use.
13. In addition to the U. T. Austin Minimum Security Standards for Systems, all Web servers providing payment card processing services must utilize the strongest transmission encryption possible (e.g., enable SSLv3 and disable SSLv2).
14. All [portable devices](#) processing payment card information (e.g., laptops, external hard drives, flash drives, CD-ROMs, DVDs) and any desktops located in physically insecure environments must implement disk [encryption](#) software. Encryption credentials must be properly escrowed, preferably using a central escrow authority, if there is a need for data retention or recovery.
15. Merchants using manual payment card processing techniques, such as point-of-sale and other credit card processing equipment, must abide by the [Office of Accounting 6.4 Handbook of Business Procedures](#).
16. The university merchant is also responsible for ensuring any credit card equipment purchased from vendors other than the university’s credit card processor (i.e., Global Payments Inc) is PCI compliant. The university merchant will coordinate proof of compliance with U. T. Austin Cash Management Services.

## 4. Additional Resources

[Supporting PCI-DSS Documents](#)

[Handbook of Operating Procedures: Credit Card Collections](#)

## 5. Revision History

Version	Date	New	Original
<b>Minimum Security Standards for Merchant Payment Card Processing</b>	3/1/2011	Converted web page to PDF	No changes.

**Minimum Security Standards for Merchant Payment Card Processing**

**Document Version:** Approved

Version	Date	New	Original
	10/1/2009	Updated visual appearance to new template. Corrected any out of date links to ensure they are pointing to the most current policy documents.	
	11/13/2007	Added link to exception process.	Unlinked.
	8/8/2007	Posting Date.	

## 6. Approvals

Name	Role	Members	Date
<b>Chief Information Security Officer</b>	Approval	Cam Beasley	March 3, 2011