



# Requirements for University Related Activities that Accept Payment Cards

MICHIGAN STATE UNIVERSITY

Requirements for University Related Activities that Accept Payment Cards

**TABLE OF CONTENTS**

**OBJECTIVE STATEMENT AND INTRODUCTION.....4**

**Compliance .....4**

**Environment .....4**

**Reference Material.....5**

**COMPLIANCE REQUIREMENTS FOR ALL MERCHANT UNITS .....6**

**Self-Assessment Questionnaire .....6**

**Document Responsibility .....6**

**Policies and Procedures .....6**

**Risk Assessment .....6**

**Awareness Program .....7**

**Restrict Access .....7**

**Protect Data .....8**

**On-going Compliance .....9**

**POLICIES AND PROCEDURES FOR ALL MERCHANT UNITS.....11**

**Document Policies and Procedures .....11**

**ADDITIONAL REQUIREMENTS FOR COMPLEX-COMPLIANCE MERCHANT UNITS..13**

**Prior Approval .....13**

**Policies and Procedures .....13**

**Self-Assessment Questionnaire .....13**

**Vulnerability Scans .....13**

**Segment Network .....13**

**Change Management .....13**

**Third-Party .....14**

**Ongoing Compliance.....14**

**ADDITIONAL POLICY AND PROCEDURE FOR COMPLEX-COMPLIANCE MERCHANT UNITS .....15**

**Technical Infrastructure .....15**

<b>Prohibition of Storing Certain Data</b> .....	15
<b>Physical Security</b> .....	15
<b>Locked Consoles</b> .....	16
<b>Payment Card Account Number Masking</b> .....	16
<b>Unreadable Stored Account Numbers</b> .....	16
<b>Secure Access</b> .....	17
<b>Password Management</b> .....	19
<b>REQUIRED DOCUMENTATION FOR COMPLEX-COMPLIANCE MERCHANT UNITS</b> ..	21
<b>Document System Management</b> .....	21
<b>Document Firewall Configuration</b> .....	23
<b>Encryption Key Management</b> .....	26
<b>Custom-Software Development Processes – Testing Guidelines</b> .....	26
<b>Custom-Software Development Processes – Secure Coding Guidelines</b> .....	28
<b>Custom-Software Development Processes – Protect Web Applications</b> .....	29
<b>Change Control</b> .....	29
<b>Backup</b> .....	30
<b>Audit Trails</b> .....	30
<b>System Clock Synchronization</b> .....	32
<b>Security Testing</b> .....	32
<b>Usage Policies</b> .....	34
<b>Incident Response Plan</b> .....	34
<b>UNIVERSITY LEVEL RESPONSIBILITIES</b> .....	36
<b>Maintain Policies</b> .....	36
<b>Annual Risk Assessment</b> .....	36
<b>Ongoing Compliance</b> .....	36
<b>Policies About Technology</b> .....	36
<b>Incident Response</b> .....	37

## OBJECTIVE STATEMENT AND INTRODUCTION

1. **Compliance** – Units that accept payment (credit/debit) cards (“Merchant Units”) must comply with this document and all the Payment Card Industry Data Security Standard (PCI DSS) requirements. 12.1.1
  
2. **Environment** – Some of the PCI DSS requirements only apply to certain card processing environments. Therefore, the University has defined two (2) types of card processing environments, based on the compliance efforts involved: simple and complex. Univ
  - 2.1 **Simple-Compliance** – A simple-compliance environment is defined as one where the Merchant Unit does not store, process or transmit cardholder data electronically. The Merchant Unit has at least one of the following: Univ
    - 2.1.1 Card swipe system not attached to a network Univ
    - 2.1.2 Paper-based process Univ
    - 2.1.3 Centrally provided payment card application (currently *webCredit*) with no unit-based electronic storage of payment card numbers Univ
    - 2.1.4 External payment card processor that has been approved by the Controller’s Office, with no unit-based electronic storage or transmission of payment card numbers Univ
  - 2.2 **Simple-Compliance Requirements** – Merchant Units with a simple-compliance environment are subject to the requirements in Sections 4-12. Univ
  - 2.3 **Complex-Compliance** – A complex-compliance environment is defined as one where the Merchant Unit does store, process or transmit cardholder data electronically on Unit-managed desktop computers or servers. The Merchant Unit has at least one of the following: Univ
    - 2.3.1 Developed or purchased computer-based systems that store, process or transmit payment card data 6.3  
6.4

- 2.3.2 Contracted with a payment card acceptance/processing/service entity outside the University or any other external entity that shares the Merchant Unit’s cardholder data (such as web hosting services, security service providers, backup media storage facilities, events managers, etc.) 12.8
- 2.3.3 Stored cardholder data that includes payment card account numbers on unit-controlled networked systems (including but not limited to storage in spreadsheets, word processing documents, imaging systems, networked fax servers, billing systems, accounting systems, contact databases, etc.) Univ
- 2.4 **Complex-Compliance Requirements** – In addition to the Compliance Requirements for All, Merchant Units with a complex-compliance environment are also subject to the requirements in Sections 13-42. Univ
3. **Reference Material** – The Payment Card Security Standards Council (PCI SSC) is an independent body that was established to govern the security standards for the payment card industry. Further clarification of any of these requirements, as well as the two documents noted below, can be found on the PCI SSC website at [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml). Univ
- 3.1 **PCI DSS** – The most current version of the PCI DSS as it relates to a particular section is referenced throughout this document. As of version 1.2, the stand-alone PCI DSS has been replaced by the audit guide referenced below. Univ
- 3.2 **PCI DSS Requirements and Security Assessment Procedures** – This audit guide incorporates the PCI DSS with additional clarification and Merchant Units are encouraged to become familiar with it. Auditors from both MSU Internal Audit and external auditing companies will use this guide for onsite PCI compliance audits. Univ

**COMPLIANCE REQUIREMENTS FOR ALL MERCHANT UNITS**

- |     |   |              |
|-----|---|--------------|
| 4.  | <b>Self-Assessment Questionnaire</b> – Complete the questionnaire annually. The simple-compliance environment questionnaire is less involved than the complete questionnaire for complex-compliance environments. | Univ         |
| 5.  | <b>Document Responsibility</b> – Document in writing who (specific positions or persons) is responsible for:  |              |
| 5.1 | Payment card data security in the unit  | 12.4<br>12.5 |
| 5.2 | Creating and distributing security policies and procedures  | 12.5.1       |
| 5.3 | Monitoring and controlling all access to payment card data  | 12.5.5       |
| 5.4 | Reporting suspected breaches to the Controller’s Office   | 12.9         |
| 6.  | <b>Policies and Procedures</b> – Maintain and follow written merchant unit policies and operational procedures for payment card acceptance and related processes, and informs employees what is expected of them. | 12<br>12.2   |
| 6.1 | For purposes of this document, “employees” refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are “resident” on the university site.             | 12           |
| 6.2 | These must meet all criteria identified as “Policies and Procedures for All Units” in Section 12 of this document.  | 12.2         |
| 6.3 | Review all required payment card related policies, procedures and documentation, at least once per year and when practices change, and update these as needed.  | 12.1.3       |
| 7.  | <b>Risk Assessment</b> – Perform a formal, written risk assessment for payment card operations at least once per year, or when procedures or technology change.   | 12.1.2       |
| 7.1 | Documentation of the risk assessment should be retained in a secure location for the current fiscal year plus the two (2) most recent fiscal years.   | Univ         |
| 7.2 | This risk assessment must include systematically reviewing processes and procedures to:   | 12.1.2       |

7.2.1	Identify valuable cardholder-related resources such as systems, data or documents	Univ
7.2.2	Identify possible threats to those resources	12.1.2
7.2.3	Quantify potential for threats to those resources – such as loss, theft, misuse or exposure – by estimating likelihood or frequency of threat along with cost of occurrence	12.1.2
7.2.4	Recommend process or policy changes that reduce risk based on threats	12.1.2
7.2.5	Define in writing, security responsibilities for all employees and contractors or other non-consumers who have access to payment card data, including password procedures and policies (“Non-consumers” are employees, volunteers, contractors, etc. – anyone other than the Merchant Unit’s customers)	12.1 12.4 8.5.7
8.	<b>Awareness Program</b> – Maintain a cardholder data security awareness program that:	12.6
8.1	Trains all employees about cardholder data security at inception of duties involving cardholder data, and at a minimum, annually	12.6.1
8.2	Requires employees to acknowledge in writing or electronically that they have read and understood University and departmental payment card data security policies and procedures	12.6.2
8.3	Uses multiple methods of communicating awareness and educating employees (posters, letters, meetings, web-based training, email reminders)	12.6.1
8.4	Records (logs) significant awareness initiatives, and records individual participation in annual training	12.6.2
9.	<b>Restrict Access</b> – Ensure that critical data can only be accessed by authorized personnel using acceptable and secure methods.	7.

9.1	Prior to hire or otherwise engaging for work, screen potential volunteers and employees (see definition of “employees” at section 6.1) who will have access to more than one card number at a time. (Note: University background checks for regular employees are sufficient to meet this requirement; Merchant Units who utilize student or other non-regular employee types are responsible for obtaining a screening of those individuals.) For those employees such as cashiers who only have access to one card number at a time, this requirement is a recommendation only.	12.7
9.2	Remove access to payment card related systems or data immediately when employees, contractors or volunteers cease duties related to payment cards.	8.5.4
9.3	Review payment card system access at minimum quarterly and remove/disable inactive or unneeded access for employees, contractors or volunteers.	8.5.5
9.4	Require a unique personal (i.e., non-shared) user ID for any employee, contractor or volunteer whose duties include access to payment card related systems or data.	8.1 8.5.8
9.5	Prohibit non-consumer use of wireless communications or technologies to access payment-card-related computer systems.	4.1.1
9.6	Prohibit solicitation of payment card data from customers via end-user messaging technologies (for example, email, instant messaging, chat)	4.2
9.7	Prohibit sending payment card account numbers (such as between staff members or to outside entities) by end-user messaging technologies, unless the cardholder data is strongly encrypted.	4.2
10.	<b>Protect Data</b> – Protect data anywhere it is stored.	3.
10.1	Appropriately secure all records that include cardholder data, including physical security of paper and electronic media (including computers, removable electronic media, networking and communications hardware, telecommunication lines, receipts, reports, faxes, etc.) in any locations where stored or used, such as desks, workspaces, file cabinets, etc.	3. 9.6
10.2	Prohibit storage of cardholder data that includes payment card account number on any networked system (including desktop systems).	12.3.10

---

10.3	Prohibit copy, move and storage functions (such as the use of cut and paste, print-to-disk, and storing) of such cardholder data to hard drives, laptops, or removable electronic media.	12.3.10
10.4	Install, and keep current via automatic updates, anti-virus software on any computers used to access <i>webCredit</i> or external payment card processing systems. Such programs must be capable of detecting, removing and protecting against all known types of malicious software, such as viruses, worms, trojans, rootkits, adware, and spyware.	5.1 5.1.1 5.2
10.5	Run regular, scheduled anti-virus scans on any computers used to access <i>webCredit</i> or external payment-card processing systems, with audit log generation enabled.	5.2
10.6	Report any suspected exposure (to unauthorized parties) or loss of cardholder data to Controller’s Office immediately.	12.9
10.7	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, including:	12.8
10.7.1	A list of all service providers	12.8.1
10.7.2	Obtain a written agreement from existing third parties with access to cardholder data to adhere to PCI DSS requirements and acknowledge that the service providers are responsible for the security of cardholder data the service providers possess or handle. (Boilerplate contract language is available from the Controller’s Office.)	12.8.2
10.7.3	Contact the Controller’s Office for guidance regarding the established process for engaging new service providers.	12.8.3
10.7.4	Maintain a program to monitor the PCI DSS compliance status of all service providers with access to cardholder data.	12.8.4
11.	<b>On-going Compliance</b> – Cooperate with University efforts to maintain compliance.	Univ
11.1	Respond to periodic questionnaires or surveys when requested by the Controller’s Office, to confirm the Merchant Unit’s ongoing PCI DSS compliance.	Univ

11.2	Assume responsibility for the cost to become and continue being compliant.	Univ
11.3	Assume responsibility for payment card industry financial penalties that may arise out of Merchant Unit non-compliance with PCI DSS requirements.	Univ
11.4	Assume responsibility for an allocated portion of University costs related to PCI DSS compliance.	Univ

**POLICIES AND PROCEDURES FOR ALL MERCHANT UNITS**

- |        |   |                              |
|--------|---|------------------------------|
| 12.    | <b>Document Policies and Procedures</b> – Merchant Units (with either simple or complex-compliance environments) must establish and follow policies and procedures covering all aspects of their payment card processing, and document these in writing. At minimum, such policies and procedures must include:   | 12.                          |
| 12.1   | <b>Payment Methods</b> – Identification of all methods by which payment card information may be received, and proper handling procedures for each method. (For example, methods might include U.S. mail, telephone, in person, fax, etc.)   | Univ                         |
| 12.2   | <b>Storage</b> – Acceptable means and methods of recording, writing down or storing cardholder information, with storage and security procedures for each method. Such procedures should include storage and labeling practices (such as numbering paper documents) that will allow the Merchant Unit to detect missing forms or media. Cardholder data storage should be kept to a minimum.      | 3.1<br>9.6                   |
| 12.2.1 | Prohibition of storing the card validation code (3 or 4 digit value printed on the front or back of the card, used to verify card-not-present transactions) in any form or location.  | 3.2.2                        |
| 12.2.2 | Definition of legitimate “need to know” for payment card numbers and other cardholder data for Merchant Unit, i.e., which positions or duties justify “need to know” and why.   | 7.1<br>7.1.1<br>7.1.2        |
| 12.2.3 | Procedures for strict control, if the Merchant Unit needs to send cardholder data to other locations inside or outside the University, for sending such data, including logging and management authorization for the transmittals, classification of the media so that it can be identified as “confidential”, and use of secure courier or other delivery method that can be accurately tracked. | 9.7<br>9.7.1<br>9.7.2<br>9.8 |
| 12.3   | <b>Retention</b> – How long and in what form payment card data may be retained by the merchant Unit, along with regular purging schedules and procedures for securely removing older data.  | 3.1                          |
| 12.3.1 | Document any legal, regulatory, or business reason(s) for retaining payment card data for the period of time it is kept.  | 3.1                          |

12.3.2	Data must be inventoried at least annually to ensure data that should be stored is still present (not lost or stolen), and is stored securely. A record/log of the periodic inventories must be maintained (date and who performed the inventory).	9.9.1
12.4	<b>Purge</b> – At minimum quarterly, outdated cardholder data must be purged according to the retention schedule, or data stores must be reviewed to verify that cardholder data has not been retained longer than documented need.	3.1 9.10
12.4.1	A record/log of these periodic purgings should be maintained (date and who performed the inventory).	3.1
12.4.2	Hardcopy materials to be purged should be physically secured until they are destroyed (for example, in a locked bin), and should be destroyed by being cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.	3.1 9.10.1
12.4.3	Cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).	3.1 9.10.2

---

## ADDITIONAL REQUIREMENTS FOR COMPLEX-COMPLIANCE MERCHANT UNITS

- |      |  |                |
|------|--|----------------|
| 13.  | <b>Prior Approval</b> – Merchant Units that plan to have a complex-compliance environment MUST contact the Controller’s Office before entering into any of the scenarios listed in 2.3.  | Univ           |
| 13.1 | The Controller’s Office will provide guidance on the process for engaging service providers, including proper due diligence prior to engagement.   | Univ<br>12.8.3 |
| 13.2 | Units that want to begin accepting payment cards or add on functionality of an existing arrangement with a third party will not be allowed to use a service provider or third-party application that is not currently validated as being PCI DSS-compliant. Furthermore, use of the new function, application or service must not require the Merchant Unit to electronically store or transmit cardholder data. | Univ<br>12.8.3 |
| 14.  | <b>Policies and Procedures</b> – Maintain and follow written Merchant Unit policies and operational procedures for payment card acceptance and related processes.  | 12.2           |
| 14.1 | These must meet all criteria covered in Sections 13-42.  | 12.2           |
| 14.2 | Review all required payment card related policies, procedures and documentation, at least once per year and when practices change, and update these as needed.   | 12.1.3         |
| 15.  | <b>Self-Assessment Questionnaire</b> – Complete a full PCI DSS self-assessment questionnaire annually. Contact Cashier’s Office for online access.   | Univ           |
| 16.  | <b>Vulnerability Scans</b> – Submit to and pay for external vulnerability scanning of payment card systems and sub-networks as required by PCI DSS, at minimum quarterly.  | 11.2           |
| 17.  | <b>Segment Network</b> – Maintain payment card related systems on a sub-network segmented to limit scanning requirements to payment card related unit-based systems. (Network configuration guidance is available from Academic Computing & Network Services Network Security group. See also subsequent sections of this document.)   | 1.1.3          |
| 18.  | <b>Change Management</b> – Ensure changes to payment card environment are handled properly.  | 11.2           |

- |      |   |                |
|------|---|----------------|
| 18.1 | Obtain Controller’s Office approval for significant changes of configuration of payment card processing or storage hardware, software or network, such as changes of operating system environment or new software vendor. Software version changes should be reported to the Controller’s Office.   | 1.1.1          |
| 18.2 | Carry out vulnerability scanning, either by the University’s qualified external scanning vendor or by internal University staff, after any significant change in the payment card environment (such as new system components, network topology changes, firewall rule modifications, product upgrades).   | 11.2           |
| 19.  | <b>Third-Party</b> – Merchant Units that contract with a payment card acceptance/ processing/service entity outside the University must ensure, via written agreement, that that entity is compliant with PCI DSS requirements and acknowledges their responsibility for securing cardholder data. The Controller’s Office can provide boilerplate contract language.   | 12.8<br>12.8.2 |
| 20.  | <b>Ongoing Compliance</b> – Review PCI DSS requirements and audit guidelines in full, and comply with all PCI DSS requirements applicable to the Merchant Unit’s technical and systems management environment, including requirements for written policies and procedures. Any exceptions must be approved by the Controller’s Office, based on the University’s payment card processor accepting alternate control measures. | 12.1.1         |

---

**ADDITIONAL POLICY AND PROCEDURE FOR COMPLEX-COMPLIANCE  
MERCHANT UNITS**

- |      |  |       |
|------|--|-------|
| 21.  | <b>Technical Infrastructure</b> – In addition to policy and procedure requirements for all Merchant Units, units with computer-based systems that store, process or transmit payment card data must also establish and follow policies and procedures covering all relevant aspects of their payment card technical infrastructure, and document these in writing. At minimum, such policies and procedures must include all items listed in this section. | Univ  |
| 22.  | <b>Prohibition of Storing Certain Data</b> – Prohibit storing in any location, including databases, incoming transaction files, history files, trace files, all logs (transaction, audit, history, debugging, error, etc.), etc., any of the following:  | 3.2   |
| 22.1 | The full contents of any track from the magnetic stripe (from the back of the card, a chip in the card, or elsewhere). Note that certain individual data elements from the stripe may be stored, specifically the accountholder name, the account number, the expiration date, and/or the service code.  | 3.2.1 |
| 22.2 | The card validation code (3 or 4 digit value printed on the front or back of the card, used to verify card-not-present transactions) in any form or location.  | 3.2.2 |
| 22.3 | The PIN (personal identification number) or PIN block.   | 3.2.3 |
| 23.  | <b>Physical Security</b> – A secure physical cardholder data environment for payment card network and system components, including:  | 9     |
| 23.1 | Access controlled at all times via devices such as badge readers, lock and key, etc.   | 9.1   |
| 23.2 | Video cameras or other access control mechanisms, which are protected from tampering, in place to monitor individual physical access to sensitive areas, with video stored for at least three (3) months unless otherwise restricted by law.   | 9.1.1 |
| 23.3 | Documented procedures, such as issuance of badges that help personnel easily distinguish employees (including contractors or other persons performing onsite work on an ongoing, regular basis) from visitors (including vendors or service personnel) who enter the facility for a short duration.  | 9.2   |

23.4	Documented procedures for ensuring that all visitors to areas where cardholder data is processed or maintained are:	9.3
23.4.1	Authorized before entering these areas.	9.3.1
23.4.2	Given a physical token (such as a badge or access device) that distinguishes them from employees with regular authorized access to these areas, and that expires.	9.3.2
23.4.3	Asked to surrender the token before leaving these areas, or at the expiration date.	9.3.3
23.4.4	Recorded in a visitor log for physical access to these areas. This log should contain at minimum the visitor’s name, firm represented, and the employee authorizing physical access. Logs must be retained for a minimum of three (3) months, unless otherwise restricted by law.	9.4
23.5	Restricted physical access to network jacks with access to the payment card environment. Jacks in areas where visitors may be unescorted (such as conference rooms) should be are enabled only when and where needed by authorized employees.	9.1.2
24.	<b>Locked Consoles</b> – Locking consoles for payment card system and network components (such as via passwords) to prevent unauthorized use.	9.1
25.	<b>Payment Card Account Number Masking</b> – Documenting which functions require viewing of full payment card number, and requiring, via policy, that payment card numbers are masked in all other cases when displayed (first six and last four digits are the maximum number of digits to be displayed). Note that this requirement does not supersede stricter requirements in place for displays of cardholder data on point of sale (POS) receipts.	3.3
26.	<b>Unreadable Stored Account Numbers</b> – Rendering sensitive cardholder data unreadable anywhere it is stored electronically.	3.4
26.1	Minimum data to be rendered unreadable is the payment card account number.	3.4
26.2	Storing only the last four (4) digits of the payment card account number does not constitute storing.	3.4

---

26.3	Acceptable means of rendering data unreadable are:	3.4
26.3.1	One-way hashes based on strong cryptography	3.4
26.3.2	Truncation or masking (that is, full account number is not stored – first six (6) and last four (4) digits are the maximum number of digits stored)	3.4
26.3.3	Index tokens and PADs, with PADs securely stored	3.4
26.3.4	Strong cryptography, with associated, documented key management processes and procedures	3.4
26.4	Data must be unreadable in all locations, including databases, data repositories, files, all logs (transaction, audit, history, debugging, error, etc.), document images, removable or backup media, etc.	3.4
26.5	If disk encryption is used (rather than file or column-level database encryption):	3.4.1
26.5.1	Logical access to encrypted file systems must be managed independently of native operating system access control mechanisms (for example, not using local user account databases or Active Directory accounts).	3.4.1
26.5.2	Cryptographic keys must be stored securely (for example, on removable media that is adequately protected with strong access controls).	3.4.1
26.5.3	Decryption keys must not be tied to user accounts.	3.4.1
26.5.4	Decryption must be stored securely and not on the local system (for example, stored on removable media that is adequately protected with strong access controls).	3.4.1
26.5.5	Removable media must also be encrypted, and encrypted separately.	3.4.1
27.	<b>Secure Access</b> – Securing access to system components used in the payment card process, and to cardholder data. Policy and process must include:	7.1

27.1	Restriction of access to the least privileges necessary to perform job responsibilities, based on job classifications and functions	7.1.1 7.2.2
27.2	Assignment of privileges is based on individual personnel's job classification and function	7.1.2
27.3	Requirement for an authorization form, signed by management that authorizes and specifies required privileges.	7.1.3
27.4	An automated access control system that covers all system components in the payment card environment.	7.1.4 7.2.1
27.4.1	To authenticate regular users, the system must require at minimum a password or passphrase, or two-factor authentication (for example, token devices, smart cards, biometrics or public keys) in addition to the access ID or account name.	8.2
27.4.2	To authenticate remote network access (network-level access originating from outside the network) to the payment card environment by employees, administrators, or third parties such as contractors or vendors, the system must require two-factor authentication, such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	8.3
27.5	Use of authorization forms to control addition, deletion, and modification of user IDs, credentials and other identifier objects.	8.5.1
27.6	An access control system for all payment card environment components that locks out users after not more than six (6) invalid password attempts, and maintains the lock for at least 30 minutes or until an administrator re-enables the user ID.	8.5.13 8.5.14
27.7	An access control system for all payment card system components that requires password re-entry if the session has been idle for more than 15 minutes.	8.5.15
27.8	Practices that ensure vendor accounts used to support and maintain system components are inactive by default, activated only when needed by the vendor, and monitored while being used.	8.5.6

27.9	Authentication of all access to any database containing cardholder data, for access by applications, administrators, and all other users.	8.5.16
27.10	Prohibition of direct access or queries to any database containing cardholder data. (Only a limited number of database administrators may have individual database login accounts.)	8.5.16
27.11	Verification that database application IDs can be used only by the application (and not by individual users or other processes).	8.5.16
27.12	A “deny all that is not specifically permitted” configuration for all components. Default setting must be set to “deny all.”	7.2 7.2.3
27.13	Documentation of firewall standards for mobile or employee-owned computers that are used to access the internet and/or the payment card sub-network must have personal firewall software installed and active. Such software must be configured by the Merchant Unit to specific documented standards, and must not be alterable by the employee.	1.4
28.	<b>Password Management</b> – Proper user authentication and password management for all users on all components of the payment card environment, including software development, network support, non-consumer users, etc.	8.5
28.1	Passwords must meet these minimum requirements:	
28.1.1	Expire at least every 90 days	8.5.9
28.1.2	Are a minimum of seven (7) characters in length	8.5.10
28.1.3	Must contain both alphabetic and numeric characters	8.5.11
28.1.4	Are not the same as any of the last four (4) passwords used for that account	8.5.12
28.2	Render all passwords unreadable during transmission and storage on all system components using strong cryptography (as defined in PCI DSS Glossary).	8.4
28.3	Verification of user identity before password is reset.	8.5.2

28.4	First-time passwords for new users that are unique per user, and required to be changed after first use.	8.5.3
28.5	Remove/disable inactive accounts at minimum every 90 days.	8.5.5

---

## REQUIRED DOCUMENTATION FOR COMPLEX-COMPLIANCE MERCHANT UNITS

- |        |   |                |
|--------|---|----------------|
| 29.    | <b>Document System Management</b> – Document system and network configuration standards, policies and procedures applicable to the unit subnet which includes payment card storage or processing systems. These standards, policies and procedures must include at minimum:   | 1.1            |
| 29.1   | Description of roles, groups, and responsibility for logical management of network components, including responsibility for maintaining up-to-date network documentation.   | 1.1.4<br>1.1.2 |
| 29.2   | A documented list of all services/ports supported on the Merchant Unit’s payment card sub-network. For protocols other than HTTP (hypertext transfer protocol), SSL (secure sockets layer), SSH (secure shell) and VPN (virtual private network), the Merchant Unit must justify and document why the protocols are necessary for business. | 1.1.5          |
| 29.3   | Additional justification for insecure protocols (generally, those other than HTTP, HTTPS, SSH, and VPN) including additional security features implemented to mitigate risk.  | 1.1.5          |
| 29.4   | Requirement for strong cryptography and security protocols when sensitive cardholder data is transmitted over open, public networks.  | 4.1            |
| 29.4.1 | Open, public networks, for purposes of this requirement, include the general campus network, the internet, GSM (global system for mobile communications), and GPRS (General Packet Radio Service).  | 4.1            |
| 29.4.2 | Acceptable encryption includes Secure Sockets Layer (SSL)/Transport Layer Security (TLS), or Internet Protocol Security (IPSEC), with proper encryption strength for the encryption methodology in use.   | 4.1            |

---

29.4.3	Proper encryption strength relies on cryptographic key. Effective size of the key should meet the minimum key size of comparable strengths recommendations. One reference for minimum comparable strength is NIST Special Publication 800-57, as updated from time to time ( <a href="http://csrc.nist.gov/publications/">http://csrc.nist.gov/publications/</a> ) or others that meet the following minimum comparable key bit security: 80 bits for secret key based systems such as TDES; 1024 bits modulus for public key algorithms based on the factorization such as RSA; 1024 bits for the discrete logarithm such as Diffie-Hellman, with a minimum 160 bits size of a large subgroup such as DSA; 160 bits for elliptic curve cryptography such as ECDSA.	4.1
29.5	Change management procedures for carrying out all changes to the production environment, including a requirement for testing and explicit documented management approval for changes to network connections and firewall and router configuration.	1.1.1
29.6	A current network diagram that documents all connections to cardholder data, and assignment of responsibility for keeping that diagram current.	1.1.2
29.7	Policy requiring review of firewall and router rule sets at least every six (6) months and assigning responsibility for that review, and procedure that includes keeping a written record that each such review has taken place and who performed it.	1.1.6
29.8	Policy requirement for and deployment of anti-virus mechanisms on all computers in the payment card process and those commonly affected by malicious software, including servers, desktops used to operate or administer systems, etc.	5.1
29.8.1	Anti-virus mechanisms should enable automatic updates and periodic scans, and logs should be retained in accordance with documented retention policy and PCI DSS Requirement 10.7.	5.2
29.8.2	Anti-virus mechanisms must be capable of detecting, removing, and protecting against all known forms of malicious software, including viruses, spyware, and adware.	5.1.1
29.9	Policy requirement and supporting procedures to ensure that all system components and software have vendor-supplied security patches installed promptly, at minimum within one month of patch release.	6.1

29.10	Documented processes and responsibilities for identifying and addressing security vulnerabilities, such as alert services. Process should include measures for updating configuration standards and configurations to address new vulnerabilities as required by PCI DSS Requirement 2.2. These processes must include use of external, expert resources (for example, CERT).	6.2
30.	<b>Document Firewall and Router Configuration</b> – Firewall and router configuration standards, policies and procedures applicable to the unit subnet which includes payment card storage or processing systems. These standards, policies and procedures must include at minimum:	1.1
30.1	The requirements for a firewall and router:	
30.1.1	Between any system component in the departmental payment card sub-network and the campus or commodity internet.	1.3
30.1.2	Between the DMZ (demilitarized zone) of the payment card sub-network and the data storage zone of the payment card sub-network.	1.1.3
30.1.3	Between the payment card sub-network zone and the Merchant Unit’s other non-payment-card sub-network(s).	1.3
30.2	Documentation of standards for network firewall configuration and router rules.	1.1
30.3	Documentation of firewall standards for mobile or employee-owned computers that are used to access the internet and/or the payment card sub-network must have personal firewall software installed and active. Such software must be configured by the Merchant Unit to specific documented standards, and must not be alterable by the employee.	1.4
30.4	Policies and procedures for installing system components that include provisions for:	2.1
30.4.1	Changing passwords from vendor-supplied defaults	2.1
30.4.2	Eliminating unnecessary accounts	2.1
30.4.3	Changing defaults for simple network management protocol (SNMP) community strings	2.1

	30.4.4	Disabling wireless access attached to cardholder environment or transmitting cardholder data	2.1.1 9.1.3
30.5		Configuration standards for all new and existing system components. These standards must:	2.2
	30.5.1	Address all known security vulnerabilities and be consistent with industry-accepted system hardening standards. Examples of industry-accepted standards are those defined by SANS (SysAdmin Audit Network Security Network), NIST (National Institute of Standards Technology) and CIS (Center for Internet Security).	2.2
	30.5.2	Require implementing only one primary function per server (e.g., web servers, database servers, and DNS should be implemented on separate servers).	2.2.1
	30.5.3	Require that all unnecessary or insecure services and protocols – services and protocols not directly needed to perform server functions – must be disabled.	2.2.2
	30.5.4	Document system security parameters, which should be configured to prevent misuse.	2.2.3
	30.5.5	Require that all unnecessary functionality (scripts, drivers, features, subsystems, file systems, servers, etc.) be removed.	2.2.4
	30.5.6	Require encryption for all web-based management and other non-console administrative access, using technologies such as SSH, VPN, or SSL/TLS. Telnet and other remote login commands must not be available for use.	2.3
30.6		Firewall/router configurations that set up a zoned sub-network that separates the payment card sub-network from the external and campus network, and further separates the payment card sub-network into a DMZ and an internal network zone.	1.3
	30.6.1	Any system component that stores cardholder data must be located on the internal network zone.	1.4
	30.6.2	Any sub-network within the unit that does not meet all standards for payment card processing must be on a separate zone from the payment card sub-network.	Univ

---

30.7	Direct route inbound or outbound traffic is not permitted between the internet or campus network and the internal network. All traffic must be filtered and screened through the DMZ to allow only protocols that are necessary for the cardholder data environment.	1.3.1 1.3.3
30.8	Outbound traffic from the internal network may only access IP addresses within the DMZ.	1.3.5
30.9	IP addresses within the internal network are restricted from being translated and revealed on the internet by use of Network Address Translation (NAT), Port Address Translation (PAT) or other technologies that implement RFC 1918 address space.	1.3.8
30.10	Firewall/router configurations that restrict connections between publicly accessible servers and any component storing cardholder data.	1.3
30.11	All traffic from “untrusted” networks and hosts must be denied by default, except for protocols required for business purposes and documented in the firewall/router policy.	1.2
30.12	Inbound Internet traffic is limited to IP addresses within the DMZ (ingress filters).	1.3.2
30.13	Internal addresses cannot pass from the Internet into the DMZ.	1.3.4
30.14	The firewall/router performs stateful inspection (also known as dynamic packet filtering), i.e., only established connections associated with a previously established session should be allowed in to the network.	1.3.6
30.15	Database must be on an internal network zone, segregated from the DMZ.	1.3.7
30.16	Inbound and outbound traffic is limited to that which is documented as necessary for the payment card environment.	1.2.1 1.1.5
30.17	Router configuration files are secured, and synchronized (for example there are identical configuration for the running configuration files and the start-up configuration files).	1.2.2
30.18	All other inbound and outbound traffic not specifically permitted is denied.	1.2.1
30.19	Traffic from wireless subnets is denied.	1.2.3

31.	<b>Encryption Key Management</b> – Processes, procedures and responsibilities for protecting cryptographic keys. Key management policies and procedures for keys used for encryption of cardholder data must include:	3.5 3.6
31.1	Restricting access to keys to the fewest number of custodians necessary, with legitimate business need-to-know documented	3.5.1
31.2	Storing keys in the fewest possible locations and forms	3.5.2
31.3	Storing key-encrypting keys separately from data-encrypting keys	3.5.2
31.4	Generating strong keys	3.6.1
31.5	Securing distribution of keys	3.6.2
31.6	Securing key storage	3.6.3
31.7	Periodic key changes, at minimum annually, as deemed necessary by the associated application (for example, re-keying)	3.6.4
31.8	Retirement or replacement of old or invalid keys, or those suspected of being compromised	3.6.5
31.9	Split knowledge and establishment of dual control of keys so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key	3.6.6
31.10	Controls to prevent unauthorized substitution of keys	3.6.7
31.11	Replacement of known or suspected compromised keys	3.6.5
31.12	Deployment of a form, to be signed by key custodians, outlining their responsibilities and specifying that they accept and understand their key-custodian responsibilities	3.6.8
32.	<b>Custom-Software Development Processes – Testing Guidelines:</b> Software development processes must be done in accordance with PCI DSS and based on industry best practices if the payment card processing environment includes software developed or modified by Merchant Unit staff or contractors. The testing guidelines for software development process must include security provisions throughout the software development lifecycle. These documented testing guidelines must include:	6.3

---

32.1	Testing of all changes (including patches and system and software configuration changes) before they are deployed in production, including but not limited to the following:	6.3.1
32.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	6.3.1.1
32.1.2	Validation of proper error handling	6.3.1.2
32.1.3	Validation of secure cryptographic storage	6.3.1.3
32.1.4	Validation of secure communications	6.3.1.4
32.1.5	Validation of proper role-based access control (RBAC)	6.3.1.5
32.2	Separation of test/development environments from the production environment, with access controls in place to enforce the separation.	6.3.2
32.3	Proper separation of duties between those personnel assigned to the development/test environments and those assigned to the production environment. Access levels and user profiles can be used to accomplish this.	6.3.3
32.4	Prohibition on real payment card account numbers being used for testing or development.	6.3.4
32.5	Removal of test data and accounts from application data before a production system becomes active.	6.3.5
32.6	Review of application accounts, usernames and passwords and removal of test-environment-specific accounts, usernames and passwords, before the system goes into production or is released for customer use. Application passwords, such as those used by the application to access a database, should not be the same in the production environment as in the test environment.	6.3.6
32.7	Review of new or modified internal and public-facing application code prior to release to production or customers in order to identify any potential coding vulnerability as part of the system development life cycle required by PCI DSS Requirement 6.3. The review (either manual or automated) must include:	6.3.7

32.7.1	Review by individual other than the originating code author who is knowledgeable in code review techniques and secure coding practices	6.3.7
32.7.2	Regarding the public-facing web applications, ensure code is developed according to secure coding guidelines, such as the Open Web Security Project Guide (see PCI DSS Requirement 6.5) and addresses ongoing threats and vulnerabilities after implementation, as defined in PCI DSS Requirement 6.6	6.3.7
32.7.3	Implementation of appropriate corrections prior to release	6.3.7
32.7.4	Management review and approval of code review results prior to release	6.3.7
33.	<b>Custom-Software Development Processes – Secure Coding Guidelines:</b> Software development processes, including software developed or modified by Merchant Unit staff or contractors must use secure coding guidelines, such as the current version of the Open Web Application Security Project (OWASP) Guidelines, be done by developers that are knowledgeable in secure coding techniques, and provide training for development staff in secure coding techniques. These coding guidelines should include provisions to address and prevent vulnerabilities from:  <i>Note: The vulnerabilities listed below were current when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.</i>	6.5
33.1	Cross-site scripting attacks	6.5.1
33.2	Injection flaws, particularly SQL, as well as other command injections	6.5.2
33.3	Malicious file execution (validate input to verify user data cannot modify meaning of commands and queries)	6.5.3
33.4	Insecure direct object references (do not expose internal object references to users)	6.5.4
33.5	Cross-site request forgery (do not reply on authorization credentials and tokens automatically submitted by browsers)	6.5.5

---

33.6	Information leakage and improper error handling (do not leak information via error messages or other means)	6.5.6
33.7	Broken authentication and session management (properly authenticate users and protect account credentials and session tokens)	6.5.7
33.8	Insecure cryptographic storage (prevent cryptographic flaws)	6.5.8
33.9	Insecure communications (properly encrypt all authenticated and sensitive communications)	6.5.9
33.10	Failure to restrict URL access (consistently enforce access control in presentation layer and business logic for all URLs)	6.5.10
34.	<b>Custom-Software Development Processes – Protect Web Applications:</b> Software development processes must be based on industry standards if the payment card processing environment includes software developed or modified by Merchant Unit staff or contractors. The development process must ensure that public-facing web applications are protected on an on-going basis against known attacks by one of the following methods:	6.6
34.1	Having all custom application code reviewed for common vulnerabilities via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.	6.6
34.2	Installing a web-application firewall in front of public-facing web-facing applications.	6.6
35.	<b>Change Control</b> – Change control procedures for all changes to system components Change control procedures must include:	6.4
35.1	Documentation of impact of each change	6.4.1
35.2	Management sign-off by authorized individuals	6.4.2
35.3	Requirement for testing that verifies operational functionality	6.4.3
35.4	Back-out procedures for each change	6.4.4

36.	<b>Backup</b> – Storage of backup media that contain cardholder data in a physically secure location, with periodic inventories to verify that data remains present, is securely stored, and that data past its retention schedule is purged. Offsite storage of backups is recommended but not required. Review the location’s security at least annually.	9.5 9.9
37.	<b>Data Purging/Destruction</b> – Secure practices for destruction of electronic media, when such media are disposed of or re-purposed, in such a way that cardholder data cannot be reconstructed, in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).	9.10.2
38.	<b>Audit Trails</b> – Tracking and monitoring all access to cardholder data and to network resources associated with the payment card sub-network. This tracking and monitoring must include:	10
38.1	A process (audit trails) for linking each access to system components to an individual user (especially for those with administrative access such as “root”).	10.1
38.2	Audit trails that allow reconstruction of the following events, for all system components:	10.2
38.2.1	All individual accesses to cardholder data	10.2.1
38.2.2	All actions taking by any individual with root or administrative privileges	10.2.2
38.2.3	Access to all audit trails (such as logs, etc.)	10.2.3
38.2.4	Invalid logical access attempts	10.2.4
38.2.5	Use of identification and authentication mechanisms	10.2.5
38.2.6	Initialization of audit logs	10.2.6
38.2.7	Creation and deletion of system-level objects	10.2.7
38.3	Audit trail entries for each event, for all system components, that include at minimum:	10.3
38.3.1	User identification	10.3.1

---

38.3.2	Type of event	10.3.2
38.3.3	Date and time	10.3.3
38.3.4	Success or failure indication	10.3.4
38.3.5	Origination of event	10.3.5
38.3.6	Identification of affected data, system component, or resource	10.3.6
38.4	Security for audit trails so that they cannot be altered in any way, including:	10.5
38.4.1	Limiting viewing of audit trails to those with a job-related need to know.	10.5.1
38.4.2	Protecting the audit trail files from unauthorized modification via access control mechanisms, physical segregation, and/or network segregation.	10.5.2
38.4.3	Prompt backups of audit trail files to a centralized log server or media that is difficult to alter.	10.5.3
38.4.4	Offloading or writing to a secure centralized internal log server or media of all logs for external-facing technologies (for example, firewalls, DNS, mail).	10.5.4
38.4.5	Use of file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (new log data being added should not cause an alert).	10.5.5
38.5	Daily review of all logs for all system components, including those servers that perform security functions like intrusion detection and authentication. Log harvesting, parsing, and alerting tools may be used to implement this requirement.	10.6
38.6	Required follow-up on any exceptions found during daily log reviews.	10.6
38.7	Retention of audit trail history for a minimum of one (1) year, with a minimum of three (3) months immediately available for analysis (for example, online, archived or restorable from back-up).	10.7

---

39.	<b>System Clock Synchronization</b> – Synchronizing all critical system clocks and time, including:	10.4
39.1	Use of NTP or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, for synchronization.	10.4
39.2	Two or three central time servers that receive external time signals (directly from special radio, GPS satellites, or other external sources, based on International Atomic Time and UTC), peer with each other to keep accurate time, and share the time with other internal servers. (Internal servers should not all be receiving time signals from external sources.)	10.4
39.3	Designation of specific external hosts from which the time servers will accept NTP time updates to prevent a malicious individual from changing the clock. Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers).	10.4
40.	<b>Security Testing</b> – Regularly and periodically testing security systems and processes to ensure that security controls continue to reflect a changing environment. Testing must include:	11
40.1	Testing of security controls, limitations, network connections and restrictions to make sure they can identify or stop any unauthorized access attempts. Tests must take place at minimum quarterly.	11
40.2	Testing with a wireless analyzer, at minimum quarterly, to ensure that no wireless access points are available in the payment card sub-network.	11.1
40.3	Verification that the Merchant Unit’s Incident Response Plan (PCI DSS Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.	11.1

- 
- |        |   |        |
|--------|---|--------|
| 40.4   | Running internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). <i>Note: Quarterly external network vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes and internal scans may be performed by the company's internal staff.</i>   | 11.2   |
| 40.5   | Timely remediation of exceptions found during security testing or in external scan results, until passing test or scan results are achieved.  | 11.2   |
| 40.6   | Internal and external penetration testing on network infrastructure and applications at least once per year, and after any significant infrastructure or application upgrade or modification (such as operating system upgrade, added sub-network, added web server, custom software modifications, etc.), and timely correction of any vulnerabilities discovered via such testing. These penetration tests must include:  | 11.3   |
| 40.6.1 | Network-layer penetration tests, including components that support network functions, as well as operating systems.   | 11.3.1 |
| 40.6.2 | Application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5.   | 11.3.2 |
| 40.7   | Use of network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and configured to alert personnel to suspected compromises. Such systems must be configured, maintained, and updated per vendor instructions to ensure optimal protection.  | 11.4   |
| 40.8   | Use of file integrity monitoring to alert personnel to unauthorized modification of critical system, configuration or content files, with comparison of critical files at least weekly. Critical files are those which do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Critical files to be monitored should include those at the operating system level, and any critical files associated with custom applications. Examples include system and application executables, configuration and parameter files, and centrally stored, historical or archived, log and audit files. | 11.5   |

40.9	Timely action on alerts generated by intrusion detection/prevention and file integrity monitoring.	11.4 11.5
41.	<b>Usage Policies</b> – For any employee-facing technologies (for example, remote-access technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email usage and Internet usage) with access to the payment card sub-network that:	12.3
41.1	Require explicit management approval to use the technology.	12.3.1
41.2	Require authentication for use of the technology.	12.3.2
41.3	Maintain a list of all such devices and the personnel with access to them.	12.3.3
41.4	Label the devices with owner, contact information, and purpose.	12.3.4
41.5	Define acceptable uses for the technology.	12.3.5
41.6	Define acceptable network locations for the technologies.	12.3.6
41.7	Are consistent with a list of Merchant Unit-approved products.	12.3.7
41.8	Have sessions that automatically disconnect after a specified period of inactivity.	12.3.8
41.9	Activate these technologies for vendors only when needed, with immediate deactivation after use.	12.3.9
42.	<b>Incident Response Plan</b> – Must be prepared to respond immediately to a breach and have an incident response plan that includes:	12.9
42.1	Immediate reporting of incidents according to University incident response procedures ( <a href="http://ict.msu.edu/documents/security-breach-guidelines.pdf">http://ict.msu.edu/documents/security-breach-guidelines.pdf</a> ), and reference to those procedures.	12.9.1
42.2	Identification of roles, responsibilities, and communication in the event of a compromise.	12.9.1
42.3	Coverage and responses for all critical system components.	12.9.1

---

42.4	Strategy for business continuity post-compromise, in the expectation that systems involved in the compromise may be unavailable in order to preserve them for forensic investigations.	12.9.1
42.5	Data back-up processes.	12.9.1
42.6	Annual testing of the plan.	12.9.2
42.7	Designation of personnel to be available on a twenty-four-hour by seven-day continuous basis to monitor for and respond to alerts and any other evidence of unauthorized activity.	12.9.3
42.8	Appropriate periodic training to staff with responsibilities related to incident management.	12.9.4
42.9	Information about monitoring and responding to alerts from intrusion detection, intrusion prevention, file integrity or other monitoring systems that may trigger or affect incident response, including unauthorized wireless access points.	11.1 12.9.5
42.10	Process to modify and evolve the incident response plan based on annual testing, experience, and to incorporate industry developments or University-level process changes.	12.9.6

**UNIVERSITY LEVEL RESPONSIBILITIES**

43.	<b>Maintain Policies</b> – Review University-level policies and procedures at minimum annually or when the environment changes.	12.1.3
43.1	Update as needed to ensure that changing business practices are represented and that the University-level policies address all requirements of the most current version of the PCI DSS.	12.1 12.1.1 12.5.1
43.2	Communicate with service providers, card associations and consultants to stay current with changing industry.	12.1
43.3	Disseminate pertinent information to all Merchant Units and relevant users.	12.1 12.5.1
44.	<b>Annual Risk Assessment</b> – Coordinate an annual risk assessment of any University-level aspects of payment card processing. This risk assessment (as defined in the PCI DSS glossary) must include systematically reviewing processes and procedures to:	12.1.2
44.1	Identify valuable cardholder-related resources such as systems, data or documents.	Univ
44.2	Identify possible threats to those resources.	12.1.2
44.3	Quantify potential for threats to those resources – such as loss, theft, misuse or exposure – by estimating likelihood or frequency of threat along with cost of occurrence.	Univ
44.4	Recommend process or policy changes that reduce risk based on threats.	Univ
45.	<b>Ongoing Compliance</b> – Document position or persons responsible within the University for coordinating University-wide PCI DSS compliance, including policies and procedures for cardholder information security, distribution of information and centralized incident response management specific to cardholder data.	12.4 12.5 12.5.1 12.9 12.9.1- 12.9.6
46.	<b>Policies About Technology</b> – Document the position or persons responsible for coordinating technical and technical-policy cardholder information security and access to cardholder data, including:	12.3 12.5 12.5.5

---

46.1	Monitoring and analyzing security alerts and information and distributing them to appropriate personnel.	12.5.2
46.2	Establishing, documenting and distributing central security incident response and escalation procedures for overall incident management.	12.5.3
46.3	Administration of user accounts (including additions, deletions and modifications) within the central authentication infrastructure used for payment card processing.	12.5.4
47.	<b>Incident Response</b> – Document the position or persons responsible for coordinating centralized payment card security incident response and escalation as prescribed in the University incident response procedures at <a href="http://ict.msu.edu/documents/security-breach-guidelines.pdf">http://ict.msu.edu/documents/security-breach-guidelines.pdf</a> .	12.5.3 12.9.1
47.1	Determine if a suspected compromise meets the criteria of a true and reportable incident.	Univ
47.2	Notify processor and card associations as appropriate.	12.9.1
47.3	Determine communication strategies, including whether cardholders will be notified and by what means.	12.9.1 Univ