Cardholder Data Information Security Policy

Version 3.1
## Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Prepared By</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft Version 1.0</td>
<td>15-Aug-12</td>
<td>ControlCase</td>
<td></td>
</tr>
<tr>
<td>Draft Version 1.1</td>
<td>25-Aug-12</td>
<td>Mary Luebke</td>
<td>Document Reformatted</td>
</tr>
<tr>
<td>Draft Version 1.2</td>
<td>21-Sept-12</td>
<td>Credit Card Acceptance Committee</td>
<td>Document revised for UWM cardholder environment and cardholder data</td>
</tr>
<tr>
<td>Final Version 1.2</td>
<td>08-Nov-12</td>
<td>Credit Card Acceptance Committee</td>
<td>Modifications made to address comments from QSA.</td>
</tr>
<tr>
<td>Draft Version 2.0</td>
<td>09-Apr-13</td>
<td>Mary Luebke</td>
<td>Revised section 2 to include only those policies and procedures we developed; Added reference to Accounting Services Procedure 2.2.23 Credit Card Acceptance.</td>
</tr>
<tr>
<td>Final Version 2.0</td>
<td>05-Aug-13</td>
<td>Mary Luebke</td>
<td>Added Hyperlinks &amp; finalized</td>
</tr>
<tr>
<td>Draft Version 3.0</td>
<td>08-Aug-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td>Update for PCI DSS 3.0</td>
</tr>
<tr>
<td>Draft Version 3.1</td>
<td>19-Aug-15</td>
<td>Credit Card Acceptance Committee</td>
<td>Annual review and update for 3.1</td>
</tr>
<tr>
<td></td>
<td>10/22/2015</td>
<td>Policy and Procedure</td>
<td>Edited to include reference to log review in section 13.1.</td>
</tr>
</tbody>
</table>

## Document Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reviewed By</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 3.0</td>
<td>24-Jul-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td></td>
</tr>
<tr>
<td>Version 3.1</td>
<td>19-Aug-15</td>
<td>Credit Card Acceptance Committee</td>
<td></td>
</tr>
</tbody>
</table>
1. Scope

This policy document provides the framework to develop and disseminate a credit card information security policy in order to achieve compliance with the Payment Card Industry Data Security Standards. This policy document is the master document, which is supported by other documents governing compliance within the University of Wisconsin-Milwaukee’s (UWM’s) credit card environment.

2. Cardholder Data Information Security Policy Coverage

*Cardholder Data Information Security Policy* of UWM encompasses:

2.1 *Access Control Policy*
2.2 *Access Control Procedure*
2.3 *Asset Classification Procedure*
2.4 *Audit Log and Monitoring Policy*
2.5 *Cardholder Data Information Security Policy (this document)*
2.6 *Data Retention, Retrieval and Secure Disposal Policy*
2.7 *Incident Management (Response Plan)*
2.8 *Key Management & Encryption Policy*
2.9 *Key Management Procedure*
2.10 *Log Review Procedure*
2.11 *Media Policy & Procedure*
2.12 *Network Device Configuration Standards*
2.13 *Patch Management and Malicious Code Prevention Policy*
2.14 *Patch Management Procedure*
2.15 *Physical Access Control Policy*
2.16 *System Configuration Standards*
2.17 *Technology Usage Policy*
2.18 *Vulnerability Management Policy*
2.19 *Vulnerability Scanning Procedures*
3. Policy Dissemination

The cardholder data information security policy must be published and disseminated to all relevant cardholder data system users (including vendors, contractors, and business partners). [SAQ Req. #1.5, #2.5, #3.7, #4.3, #5.4, #6.7 #7.3, #8.8, #9.10, #10.8, #11.6 and #12.1] - //10.8 change does not affect us.

4. Risk Assessment

UWM will perform an annual risk assessment process that would identify major strategic developments in the industry, emerging threats, & vulnerabilities, to business and Information Technology (IT) cardholder data assets of UWM and report results in a formal risk assessment document. Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30. [SAQ Req. #12.2]

5. Cardholder Data Information Security Policy Review

The cardholder data information security policy will be reviewed by the Credit Card Acceptance Committee at least annually and updated as needed to reflect changes to business objectives or the risk environment. [SAQ Req. #12.1.1]

6. Cardholder Data Information Security Policy Responsibilities

The cardholder data information security policy will define the position(s) responsible for implementing and maintaining information security throughout the cardholder data environment. [SAQ Req. #12.4] //12.4.1 does not affect us

6.1 Establish, document, and distribute security policies and procedures. [SAQ Req. #12.5.1]
6.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. [SAQ Req. #12.5.2]
6.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. [SAQ Req. #12.5.3]

7. Formal Cardholder Data Security Awareness Program

7.1 Implement a formal cardholder data security awareness program to make all relevant personnel aware of the importance of cardholder data security through educating and communicating relevant cardholder data security policies and procedures. [SAQ Req. #12.6(a)]

7.2 Educate personnel upon hire and at least annually on relevant cardholder data security policies and procedure (for example, by letters, posters, memos, meetings, promotions and web-based training). [SAQ Req. #12.6.1(a) and #12.6.1(b)]

8. Formal Acknowledgement Cardholder Data Information Security Policies

UWM should require relevant personnel to acknowledge in writing that they have read and understood the company’s cardholder data security policies and procedures. [SAQ Req. #12.6.2]

9. Employee Screening and Background Checks

In order to minimize the risk of attacks from internal sources, potential personnel in UWM’s cardholder data environment must be screened through a defined procedure, which includes national, state or local background checks, as applicable. [SAQ Req. #12.7]

10. Third Party Service Provider Contractual Requirements

If cardholder data is shared with service providers or service providers can affect the security of cardholder data, then contractually the following is required: [SAQ Req. #12.8]

10.1 Service providers must adhere to the compliance requirements. [SAQ Req. #12.8.4]
10.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses. [SAQ Req. #12.8.2]
10.3 Obtain a written agreement about which PCI-DSS requirements are managed by each service provider, and which are managed by cardholder data merchants. [SAQ Req. #12.8.5] //ask QSA about this, do we need to delineate the specific requirements and the responsibilities per requirements
11. Connected Entity Requirements

All cardholder data processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:

11.1 Maintain list of connected entities [SAQ Req. #12.8.1]
11.2 Ensure proper due diligence is conducted prior to connecting an entity. [SAQ Req. #12.8.3]
11.3 Ensure the entity is compliant with the required standards. [SAQ Req. #12.8.4]
11.4 Connect and disconnect entities by following an established process. [SAQ Req. #12.8.3]
11.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. [SAQ Req. #12.8.5]

12. Cardholder Data Asset Classification

12.1 Cardholder data and information classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored or transmitted. The classification of the cardholder data should determine the extent to which the data needs to be controlled/secured and is also indicative of its value in terms of business assets. [SAQ Req. # 7.1.2]

12.2 The term business assets, for the purpose of the scope of this policy, refer to any cardholder data upon which the organization places a measurable value. By implication, the information is NOT in the public domain and would result in loss, damage or even business collapse, should the information to be lost, stolen, corrupted or in any way compromised.

12.3 Proper access controls and privilege levels are to be set before accessing sensitive/critical cardholder data by any user. Media containing sensitive cardholder data shall only be distributed to the authorized individuals.

12.4 All applications and equipment which are accessible to the external parties and which transmit or process sensitive/critical cardholder data should be protected by strong access control and authentication mechanisms. [SAQ Req. #9.7]

12.5 Media containing sensitive cardholder data must not be released to any external entity or third party unless authorized by the management with proper business justification.
12.6 All cardholder data, regardless of media, must be classified and identified in accordance to the Data Classification Standards. [SAQ Req. # 7.1.2]

12.7 The Data Classification Standards should be followed for the purpose of cardholder data classification. [SAQ Req. # 7.1.2]

12.8 Guidelines for cardholder data classification and sensitivity must be documented and communicated to responsible cardholder data/information owners and all support personnel in order that cardholder data receives an appropriate level of protection.

13. Roles and Responsibilities [SAQ Req. #12.4]

13.1 Information Security Officer (or equivalent)

Responsible for coordinating all aspects of cardholder information security, including but not limited to:

13.1.1 Creating and distributing security policies and procedures [SAQ Req. #12.5.1]
13.1.2 Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel. NOTE: This has been delegated to the SAITs Log Server Administrator. [SAQ Req. #12.5.2]
13.1.3 Creating and distributing security incident response and escalation procedures per UWM’s Information Incident Response Plan, which includes: [SAQ Req. #12.5.3]
   13.1.3.1 Roles, responsibilities, and communication
   13.1.3.2 Coverage and responses for all critical system components
   13.1.3.3 Notification, at a minimum, of credit card associations and acquirers
   13.1.3.4 Strategy for business continuity post compromise
   13.1.3.5 Reference or inclusion of incident response procedures from card associations
   13.1.3.6 Analysis of legal requirements for reporting compromises (for example, per Wisconsin State Statute 134.98)
13.1.4 Personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts. NOTE: This has been delegated to the SAITs Log Server Administrator. [SAQ Req. #11.4]
13.1.5 A process for evolving the incident response plan according to lessons learned and in response to industry developments per UWM’s Information Incident Response Plan [SAQ Req. #12.5.3]
13.1.6 Maintaining a formal security awareness program, for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings) [SAQ Req. #12.6]

13.1.7 Review security logs daily and follow-up on exceptions. NOTE: This has been delegated to the SAITs Log Server Administrator, as specified in the SAITs Daily PCI Operational Procedure. [SAQ Req. #10.6, #10.6.1, #10.6.2 and #10.6.3]

13.2 Merchants and/or their Information Technology Support (local and central) (or equivalent)

Shall maintain daily administrative and technical operational security procedures that are consistent with the compliance standards that include:

13.2.1 User account maintenance procedures
13.2.2 Log review procedures
13.2.3 Monitor and analyze security alerts and information and distribute to appropriate personnel [SAQ Req. #11.5(b)]
13.2.4 Administer user accounts and manage authentication [SAQ Req. #12.5.4]
13.2.5 Monitor and control all access to data [SAQ Req. #12.5.5]
13.2.6 Maintain a list of connected entities
13.2.7 Perform due diligence, with assistance from the Office of Legal Affairs and the UWM Purchasing Office, prior to connecting an entity, with supporting documentation [SAQ Req. #12.8.3]
13.2.8 Verify that the entity is compliant with the required standards, with supporting documentation [SAQ Req. #12.8.4]
13.2.9 Follow established documented purchasing procedures for connecting and disconnecting entities [SAQ Req. #12.8.3]
13.2.10 Retain audit logs for at least one year, with a minimum of three months immediately available [SAQ Req. #10.7(a)]
13.2.11 Screen potential employees to minimize the risk of attacks from internal sources

13.3 UW System Administration Internal Audit (or equivalent)

Shall be responsible for executing an audit plan that identifies threats and vulnerabilities which resulted from a formal risk assessment.

13.4 PCI Compliance Officer (or equivalent)

13.4.1 Responsible for tracking employee participation in the security awareness program, PCI Awareness Training, including:
13.4.1.1 Facilitating participation upon hire and at least annually
13.4.1.2 Ensuring that employees acknowledge in writing that they have read and understand the company’s information security policy
13.4.2 Perform required scans and penetration testing [SAQ Req. #11.2, #11.3.1, and #11.3.2]

13.5 Merchant working with Purchasing (or equivalent)

Ensure that for service providers with whom cardholder information is shared:

13.5.1 Contracts require adherence to compliance standards by the service provider [SAQ Req. #12.8.4]
13.5.2 Contracts include acknowledgement or responsibility for the security of cardholder data by the service provider [SAQ Req. #12.8.2]

14. User Access

14.1 Responsibilities

The Merchant or their IT Support is responsible for creating, documenting and maintaining individual user/user group profiles that meet the requirements of the Access Control Policy [SAQ Req. #12.5.4]

14.2 Classification of users

Users are also classified in terms of:

14.2.1 Least privileges that are necessary to perform the job responsibilities
14.2.2 Individual personnel’s job classification and function

14.3 Privileges

Privileges are allocated on a need-to-use and event-by-event basis; the request for allocation of a privilege is initiated by the user to the Merchant or their IT Support which reviews the reasons why the privilege is required and the length of time for which it is required. [SAQ Req. #7.1]
15. User provisioning and de-provisioning (creation & deletion)

User agreements contain statements of access rights and statements indicating that users have understood and accepted the conditions of access. Every user’s proposed access rights must be documented in a user form, which details the systems/services/applications/information assets, to which access is to be granted, together with the level of access that is granted, taking into account the Access Control Policy. If a user is to be granted access rights other than the standard ones set out in Access Control Policy, then the specific additional authorization of the Management is also required.

15.1 The Merchant is responsible for provisioning and deprovisioning access.

15.2 The Merchant maintains a list of authorized users, administer changes in access rights, and remove users.

15.3 Cases of attempted unauthorized access to cardholder data are subject to the UWM Acceptable Use of University Information Technology Resources Policy.

16. Password Management ///stop here, we will review

The minimum password management requirements for the systems that process, store or transmit cardholder data are as follows:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users will be issued with a temporary password, and are required to change on first login</td>
<td>o Should be mandatory for Application Access for Individual Users – Internal and External [SAQ Req. #8.2.6]</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>o Maximum password lifetime of 90 days [SAQ Req. #8.2.4(a)]</td>
</tr>
<tr>
<td>Password length</td>
<td>o Minimum of 7 characters [SAQ Req. #8.2.3(a)]</td>
</tr>
<tr>
<td>Password complexity</td>
<td>o contain at least one alphabetic and one numeric character [SAQ Req. #8.2.3(a)]</td>
</tr>
</tbody>
</table>
### Password Uniqueness
- Minimum history of 4 [SAQ Req. #8.2.5(a)]

### Period of Inactivity
- Maximum of 90 days [SAQ Req. #8.1.4]

### Storage
- Encrypted [SAQ Req. #8.2.1(a)]

### Number of failed attempts for lockout
- Maximum of 6 [SAQ Req. #8.1.6(a)]

### Lockout period
- At least 30 minutes [SAQ Req. #8.1.7]

### Session Timeout
- Maximum of 15 minutes of inactivity [SAQ Req. #8.1.8]

16.1 First-time passwords for new users are set to a unique value for each user and MUST be changed after first use. [SAQ Req. #8.2.6]

16.2 The default passwords on all new equipment in the cardholder environment are changed to conform to the UWM Cardholder Password Policy requirements (above) before the equipment is brought into production.

### User Authentication

Users are authenticated at log-on by providing both their user name and their password within the parameters of the log-on system in the cardholder environment as per section 16 of this document. [SAQ Req. #8.2]

### Review of access rights

18.1 Access rights to the cardholder environment are reviewed by the Merchant or their IT Support quarterly and their adequacy is confirmed.

18.2 User access rights to the cardholder environment are reviewed when a user’s role or location within organization changes in any way. [SAQ Req. #8.1.3]
19. Compliance

Compliance with this policy is mandatory and UWM department managers must ensure continuous compliance monitoring within their department. Compliance with the statements of this policy is a matter of periodic review by the PCI Compliance Analyst and any violation of the policy may result in corrective action as outlined in UWM Acceptable Use of University Information Technology Resources Policy.

The Vice Chancellor for Finance and Administrative Affairs is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff.

This policy was approved by the Credit Card Acceptance Committee.

This policy has been accepted by the merchant’s in each SLA. Any exception requests to this policy must be sent to the Controller’s Office for review and approval as defined in Accounting Services Procedure 2.2.23 Credit Card Acceptance.