## 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></td>
</tr>
<tr>
<td>Draft Version 1.2</td>
<td>02-Oct-12</td>
<td>Credit Card Acceptance</td>
<td>Document revised for UWM cardholder environment and cardholder data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Committee</td>
<td></td>
</tr>
<tr>
<td>Final Version 1.2</td>
<td>08-Nov-12</td>
<td>Credit Card Acceptance</td>
<td>Modifications made to address comments from QSA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Committee</td>
<td></td>
</tr>
<tr>
<td>Draft Version 2.0</td>
<td>08-Apr-13</td>
<td>Mary Luebke</td>
<td>Added reference to Accounting Services Procedure 2.2.23 Credit Card Acceptance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Version 2.0</td>
<td>05-Aug-13</td>
<td>Mary Luebke</td>
<td>Added Hyperlink &amp; Finalized</td>
</tr>
<tr>
<td>Draft Version 3.0</td>
<td>11-Sep-14</td>
<td>Credit Card Acceptance</td>
<td>Update for PCI DSS 3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Committee Designees</td>
<td></td>
</tr>
<tr>
<td>Draft Version 3.1</td>
<td>24-Sep-15</td>
<td>Credit Card Acceptance</td>
<td>Annual review and update for PCI DSS 3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Committee Designees</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10/22/2015</td>
<td>P&amp;P</td>
<td>Added 7.3 to reference 12.3.4 and added 6.4 to reference 9.9 and 9.9.3.</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>11-Sep14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td></td>
</tr>
</tbody>
</table>
1. **Scope**

The use of the University of Wisconsin-Milwaukee’s (UWM’s) cardholder data assets shall be governed by acceptable use standards and procedures according to predefined levels of sensitivity and criticality for each asset, in order to avoid loss or damage to UWM and to promote compliance with applicable law and policies.

2. **Objective**

To provide guidance to all users on the proper use of UWM’s computing resources in the cardholder data environment, including use of the Internet and email.

3. **Risk**

3.1 Users can unknowingly compromise the security, integrity and availability of UWM’s information and computing resources in the cardholder data environment through the improper use of such resources.

3.2 Any personal use of computing resources in the cardholder data environment may result in significant added costs, disruption of business processes, or any other disadvantage to the organization.

4. **Scope**

This policy applies to all users in the cardholder environment(s), including but not limited to staff, support or external personnel. It applies to the use of all systems, networks, and facilities in the cardholder data environment. Use of privately owned computers is not allowed in the cardholder data environment.

5. **General Standards**

5.1 UWM requires that the procurement of all information processing technology for the cardholder data environment be subject to a formal authorization process which considers information security. Technology includes any system(s) or device(s) that will be used to
process or store organizational information or that will connect to an organizational network or other information processing system. It includes hardware, software and services.

5.2 Critical employee-facing technologies such as critical network devices or cardholder data processing applications must include adequate authentication techniques. Proper authentication techniques must provide and archive adequate information regarding user access to critical technologies.

5.3 Access to systems in the cardholder data environment must comply with the Access Control Policy to ensure that only proper users are granted access to critical systems and information resources.

5.4 Computer systems provided by UWM are the property of UWM and are intended to be used for legitimate UWM business. Only persons authorized by UWM as "users" may access UWM’s computer systems and only to the extent that such access is required to assist them in the performance of their work. All users shall use UWM's computer systems in a professional, ethical and lawful manner in accordance with the UWM Acceptable Use of University Information Technology Resources Policy. [SAQ Req. #12.3.5]

5.5 In accordance with all UWM technology policies, wireless is not authorized in any UWM PCI environment.

5.6 USB and removable media can only be used when approved by appropriate administrative staff and only for PCI-specific uses. Credit card information can never be placed on removable media.

5.7 Any technology that is deployed for a PCI system must be placed in the proper PCI network as determined by the appropriate administrators. All new additions to the PCI network require change requests and approvals. [SAQ Req. #12.3.6]

5.8 Users must use the cardholder data technology assigned by management based on the business requirement.

6. Asset Control

6.1 Only approved hardware, software and services may be used in the cardholder data environment. Merchants and/or IT support staff must approve the products and maintain a
current list of approved products. Users are not allowed to install or use any hardware, software or services. [SAQ Req. #12.3.3]

6.2 Users must not be granted access to UWM’s systems and technologies prior to management approval. Both the user’s manager and the merchant and/or their Information Technology Support (local and central) must approve user access to critical systems especially those holding cardholder data. [SAQ Req. #12.3.1]

6.3 Access to cardholder data assets must be authenticated, including for individual users, applications, and administrators. Users and administrators are authenticated through an automated access control system using unique Identification (ID) and authentication (for example, a password) for access to the cardholder data environment. Applications must be pre-authorized to interface with the cardholder data environment. [SAQ Req. #12.3.2]

6.4 All physical devices must be inspected for tampering prior to use. Merchants are responsible for training staff on their respective point of sale devices. [SAQ #9.9 and #SAQ 9.9.3]

7. Asset Management

7.1 Merchants shall maintain an inventory of information assets. This inventory should also be used in the risk assessment process. [SAQ Req. #12.3.7]

7.2 For each asset, merchants and/or their Information Technology Support (local and central) must document sufficient information to: [SAQ Req. #12.3.4]

7.2.1 identify the asset (type or category of asset, make or manufacturer, model, serial number);
7.2.2 identify the physical (or logical) location;
7.2.3 identify the information security classification;
7.2.4 identify the business unit or business role that “owns” the asset;
7.2.5 label the asset; and,
7.2.6 identify the purpose of the asset.

7.3 Serial numbers are used as a unique identifier for asset labeling and cross-referenced with departmental documentation identifying technology group ownership, contact details, location, and purpose. [SAQ Req. #12.3.4]

8. Access Control
8.1 Any remote access must be via an encrypted channel.

8.2 Remote access sessions must be automatically disconnected after a specific period of inactivity (15 minutes or less). Remote access technologies, used for vendor access to the cardholder data network, must only be connected when required and must be immediately disconnected after use. [SAQ Req. #12.3.8]

8.3 Users accessing cardholder data remotely or locally, must not copy, move, or store cardholder data onto local hard drives, floppy disks, or other external media unless explicitly authorized for a defined business need. [SAQ Req. #12.3.10(a)]

8.4 For vendors, access should be justified, temporary, and approved by the merchant and/or their Information Technology Support (local and central). The merchant along with their Information Technology Support (local and central) should review the users having external connections to the cardholder data network on regular basis in order to disable any unnecessary access. Within one business day of the authorized access expiration date, action should be taken to remove or at least disable any remote access to the cardholder data environment. [SAQ Req. #8.1.5(a) and #12.3.9]

9. Application Control

9.1 End-User Messaging Technology

Cardholder data may not be transmitted using end-user messaging technologies (i.e., e-mail, instant messaging, chat, etc.). [SAQ Req. #4.2(b)]

9.2 File Transfer Protocol (FTP)

The use of unsecured file transfers is prohibited.

10. 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.*