### 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>22-Aug-12</td>
<td>Mary Luebke</td>
<td>Document Reformatted</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>09-Apr-13</td>
<td>Mary Luebke</td>
<td>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>22-Aug-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 3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Committee Designees</td>
<td></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>22-Aug-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td></td>
</tr>
<tr>
<td>Version 3.1</td>
<td>24-Sep-15</td>
<td>Credit Card Acceptance Committee Designees</td>
<td></td>
</tr>
<tr>
<td>Version 3.1</td>
<td>09/08/2016</td>
<td>Robert Wagner</td>
<td></td>
</tr>
</tbody>
</table>
1. Scope

This policy refers to all electronic and paper cardholder data. As of the date of this policy, the University of Wisconsin-Milwaukee (UWM) does not nor shall not store any electronic cardholder data in their environment unless specifically approved by the Controller’s Office as defined in Accounting Services Procedure 2.2.23 Credit Card Acceptance. If someone becomes aware of the electronic storage of cardholder data, they are to immediately notify the PCI Compliance Officer.

All cardholder data must be destroyed or disposed of when no longer needed according to the Data Retention, Retrieval and Secure Disposal Policy. To support this procedure, data owners must review the continued value and usefulness of cardholder data on a periodic basis.

2. Guidelines

2.1 In the event that cardholder data is formally approved/authorized to be stored, procedures shall be established and implemented for secure disposal of media containing cardholder data. This includes all electronic storage equipment being traded in, returned on end of lease/rental, donated or thrown away, regardless of the value of the asset. Storage of credit card data should be kept to a minimum. Requirements for the storage of credit card data are explained in the Accounting Services Procedure 2.2.23 Credit Card Acceptance.

2.2 All cardholder data media should be disposed of securely and safely.

2.3 Items that may require secure disposal include:

   2.3.1 Hard copy documents
   2.3.2 Voice recordings
   2.3.3 Input and output reports
   2.3.4 Magnetic tapes
   2.3.5 Computer hard disks
   2.3.6 Removable storage devices including Compact Discs (CDs), Digital Video Discs (DVDs), USB drives, etc.
   2.3.7 Program listings
   2.3.8 Test data (SAQ. Req. #6.4.4)
   2.3.9 System documentation
   2.3.10 Network equipment configuration
3. Destruction of Hardcopies

All document hardcopies no longer needed, that contains cardholder data must be destroyed in a secure way, using approved equipment and procedures, so that data cannot be recovered. Destruction must be conducted using one of the methods below: [SAQ Req. #9.8(a), #9.8(b), #9.8.1(a)]

3.1 Cross-cut Shredding
3.2 Pulping
3.3 Incineration

The responsibility for the safe destruction lies with the data owner.

4. Destruction of Information in Electronic Form

Cardholder data stored in electronic form that is no longer needed must be destroyed in a secure way, using approved equipment and procedures, so that data cannot be recovered. [SAQ Req. #9.8(a), #9.8(b), SAQ Req. #9.8.2]

5. Destruction of Cardholder Data Information

5.1 Before destroying any document or file in hardcopy or electronic form, that contains cardholder data, it must first be verified that all pages and attachments are present and complete.

The data owner must retain a record of destruction for cardholder data that will include as a minimum:

5.1.1 Date of destruction
5.1.2 The name of the person carrying out the destruction
5.1.3 The name of the data owner
5.1.4 The destruction method followed.

5.2 The above record must be maintained according to the Data Retention, Retrieval and Secure Disposal Policy.
5.3 Retention of Classification until Destruction

Documents in hardcopy and electronic form, which contain cardholder data and are to be destroyed, must be stored in physically secure areas and separately from documents (also to be destroyed) with lower classification. [SAQ Req. #9.8.1(b)]

5.4 Responsibility for Document Destruction

5.4.1 Documents in hardcopy or electronic form that contain cardholder data must be returned to their data owner to be destroyed. Destruction may be imposed by:

5.4.1.1 Instructions by the Senior Management.
5.4.1.2 Asset retention and disposal schedule.

5.4.2 Destruction of documents in hardcopy or electronic form that contain cardholder data must be conducted under the strict supervision of an authorized employee or service with the appropriate access rights. The authorized employee or service must escort the material to the location to be destroyed and ensure that destruction is carried out successfully.

6. Computer Media Handling and Destruction

6.1 Use of Storage Media and Peripheral Devices

The use of storage media and peripheral devices (e.g. DVD writers, Universal Serial Bus (USB) ports, flash disks etc.) must be limited (to the maximum extent possible) so as to cover business needs only. Centralized mechanisms that control and limit the use of such devices must be considered. Cardholder data stored on these devices must be encrypted. Employees must only use the storage media (e.g. floppy disks, USB disks etc.) provided by the University of Wisconsin-Milwaukee (UWM).

6.2 Computer Storage Media Handling

All computer storage media containing cardholder data must be handled according to the classification level of the information that they contain.

6.3 Storing Information of Different Classification in the Same Media
Information of different classification levels on the same storage media (including backups) must be stored at the highest classification.

6.4 Storage Media Transportation

The approval of the data owner is required to transport storage media that contains cardholder data outside the premises of UWM. The cardholder data on the storage media must be encrypted. [SAQ Req. #9.6.3]

**Exception:** Backup copies taken as part of the *Disaster Recovery Plan* are excluded from this statement.

6.5 Deletion Prior to Destruction, Disposal or Reuse

Magnetic or optical storage media that contains cardholder data must first be securely deleted or wiped prior to their destruction, disposal or reuse (e.g. the reuse of the personal computer hard disk) [SAQ Req. #9.8.2].

6.6 Check Prior to Destruction of Computer Media

The integrity of the content must first be verified before destroying any computer media that contains cardholder data. Specifically, special attention must be paid in case the content of the computer media is only one part of the information, for example is part of big file that is stored in two different media.

6.7 Approval for Computer Storage Media Destruction

Employees must not destroy or dispose computer storage media that contain cardholder data without prior approval by the data owner.

6.8 Approved Methods of Disposing Media

The approved methods of safely disposing information-systems media containing cardholder data are the following: [SAQ Req. #9.8.1(a) and #9.8.2]

6.8.1 Physical destruction (e.g. cross-cut shredding, shattering, incineration, pulverizing).
6.8.2 Demagnetization (or degaussing) for diskettes, hard disks or other magnetic media.
6.8.3 Overwriting using approved Department of Defense (DoD) Standards.
Exception: An exception to this policy is the storage media (e.g. magnetic tapes) used as backup media. These storage media can be re-used to store other backups of the same classification level without prior destruction of their contents.

6.9 Disposed /Destroyed Media Record

Every data owner must maintain a record detailing all the disposed of / destroyed media that contained cardholder data.

6.10 Back-up Storage Media

All backup storage media, such as backup tapes, must be marked with the classification label that has been assigned to the originating information. Backup storage media containing backups of cardholder data and which are stored off-site, must have their contents encrypted.

7. General Procedures

7.1 Important:

7.1.1 In case of equipment disposal; the procedures in the Data Retention, Retrieval and Secure Disposal Policy must be followed.

7.2 Desktops & Laptops

7.2.1 If the computer is to be transferred to another employee, the drive must be securely wiped per DoD Standards.
7.2.2 In case of hardware problems, computers must be examined on the UWM premises by the vendor.
7.2.3 If vendors require the equipment to be examined at their premises, hard drive must be securely wiped per DoD Standards or removed from the computer and reinstalled when the desktop is back to UWM premises.
7.2.4 If the issue is a physical disk problem, and the disk is under warranty a replacement should be negotiated with the vendor, the vendor can only examine the disk at UWM premises. The failed disk must be securely disposed.
7.2.5 If the disk is not under warranty, a replacement should be acquired and the failed disk must be securely disposed.
7.2.6 If the computer is to be donated or retire service at UWM, the data must be securely destroyed prior to leaving the control of the data owner.

7.2.7 Employees using desktops and laptops, must adhere to the UWM Acceptable Use of University Information Technology Resources Policy which then includes unit IT policies.

7.2.8 Under no circumstances should the password of the user’s account be provided to a vendor or anyone else.

7.3 Servers

7.3.1 In case of hardware problems, servers must be examined on UWM premises by the vendor.

7.3.2 If vendors require the equipment to be examined at their premises, hard drive must be securely wiped per DoD Standards or removed from the server and reinstalled when the desktop is back to UWM premises.

7.3.3 If the issue is a physical disk problem, and the disk is under warranty a replacement should be negotiated with the vendor, the vendor can only examine the disk at UWM’s premises. The failed disk must be securely wiped and disposed.

7.3.4 If the disk is not under warranty, a replacement should be acquired and the failed disk must be securely disposed.

7.3.5 If the server is to be donated or retire service at UWM the data must be securely destroyed prior to leaving the control of the data owner.

7.4 Routers, Switches, Firewalls, and other networking equipment.

7.4.1 Network equipment should be examined at UWM’s premises.

7.4.2 All data and information is to be physically erased from all non-volatile memory.

7.4.3 Reset the device to the factory default.

7.4.4 Confirm that no data is still retained in non-volatile memory of the device.

7.5 Leased/Rented hardware

7.5.1 All information stored on leased/rented equipment should be cleansed before being sent back to the vendor. Leased/rented hardware includes but not limited to servers, desktops, laptops, printers, and network equipment.

7.6 CD/DVD Media/Documentation

7.6.1 Destruction of optical media must be destroyed using CD/DVD shredder.

7.6.2 Flash/USB drives must be wiped per DoD Standards.
8. Compliance

Compliance with this procedure is mandatory and UWM department managers must ensure continuous compliance monitoring within their department. Compliance with the statements of this procedure is a matter of periodic review by the PCI Compliance Analyst and any violation of the procedure 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 procedure 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 procedure was approved by the Credit Card Acceptance Committee.

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