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-09</td>
<td>ControlCase</td>
<td></td>
</tr>
<tr>
<td>Draft Version 1.1</td>
<td>28-Jan-13</td>
<td>Mary Luebke</td>
<td>Document Reformatted</td>
</tr>
<tr>
<td>Draft Version 1.2</td>
<td>08-Mar-13</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-Apr-13</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>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>Finalized</td>
</tr>
<tr>
<td>Draft Version 3.0</td>
<td>15-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>06-Aug-15</td>
<td>Credit Card Acceptance Committee Designees</td>
<td>Annual review and v3.1 update</td>
</tr>
<tr>
<td>Draft Version 3.2</td>
<td>22/10/2015</td>
<td>Bob Wagner</td>
<td>Added reference to SAQ 11.5 and 11.5.1, in section 9.2</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>15-Aug-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td></td>
</tr>
<tr>
<td>Version 3.1</td>
<td>06-Aug-15</td>
<td>Credit Card Acceptance Committee Designees</td>
<td></td>
</tr>
<tr>
<td>Version 3.1</td>
<td>10/22/2015</td>
<td>P&amp;P Team</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

All of the University of Wisconsin-Milwaukee (UWM) cardholder data environment system components including, but not limited to infrastructure equipment, applications and information systems are subject to this policy.

2. Roles and Responsibilities

2.1 The merchant IT support team, in conjunction with the Information Security Office, will identify the type and level of audit logging and monitoring that might be required for each individual information asset.

2.2 The merchant IT support team is responsible for configuring the information systems to meet the requirements of this policy.

2.3 The log server administrator is responsible for building and configuring the logging environment outside of the PCI in-scope row in the DC. The log server administrator will install and configure the automated logging tool (e.g. SIEM) and hand out all access as needed to view logs, generate reports, etc. This group reviews the output of the logging tool for activity performed by the other administrators to make sure they have not performed any inappropriate activity. See the Segregation of Duties document for further responsibilities.

3. Audit Logging and Monitoring

3.1 Audit logs generated by system components for which user activity audit logging is configured should be reviewed daily and follow-up on exceptions and anomalies is required. Log harvesting, parsing, and alerting tools may be used to achieve compliance with requirement #10.6. [SAQ Req. #10.6.1(b) and 10.6.3(b)]

4. Protection of Log Information

4.1 The central log server(s) shall be configured and installed on an internal network and protected by a firewall.

4.2 Administrators are prohibited from disabling logging activity, disabling audit logs or tampering with audit log information without formal approval from Information Security.
4.3 All logs must be protected from tampering by all users.

5. Administrator and operator logs

5.1 Audit logs generated by servers/systems/devices must also contain administrator/operator activities. [SAQ Req. #10.2.2]

5.2 System administrators are prohibited from erasing or de-activating log activities. Any evidence of system misuse is reported to the Information Security Office who investigates further. [SAQ Req. #10.5.2]

5.3 Logs are to be stored on a live data source for a minimum period of 3 months; and offline for a minimum period of 1 year in a read-only state. [SAQ Req. #10.7(b) and 10.7(c)]

5.4 Audit logs should be classified as confidential and must be handled according to the Data Classification Standards. This data will only be shared with individuals who have a business need to know within the university and with third parties for support and troubleshooting purposes. A confidentiality agreement must be in place for all employees that have access to this data. Existing agreements will be amended at the earliest opportunity to reflect this policy.

6. Audit Log Requirements

6.1 Audit logging must be enabled on all critical systems in the cardholder data environment.

6.2 Audit logs generated by servers/systems/devices must log:
   6.2.1 All individual access [SAQ Req. #10.1 and #10.2.1]
   6.2.2 All root and administrative actions. [SAQ Req. #10.2.2]
   6.2.3 All failed and invalid login attempts. [SAQ Req. #10.2.4]
   6.2.4 The identification or authentication mechanism used to provide access to a user in the in scope environment including, but not limited to creation of new accounts, and elevation of privileges. [SAQ Req. #10.2.5]
   6.2.5 Initialization, stopping or pausing of audit logs. [SAQ Req. #10.2.6]
   6.2.6 Creation of system level objects. [SAQ Req. #10.2.7]
   6.2.7 All access to the audit logs. [SAQReq. #10.2.3]
6.3 The audit trail entries for all system components must record the following: [SAQ Req. #10.3]
   6.3.1 User identification
   6.3.2 Type of event
   6.3.3 Date and time
   6.3.4 Success or failure indication
   6.3.5 Origination of event
   6.3.6 Identity or name of affected data, system component, or resource

6.4 Access to the audit trail must be restricted to only individuals who have a job related need to view audit trail files. [SAQ Req. #10.5.1]

6.5 Audit log files must be protected from unauthorized modifications using physical separation or access control. [SAQ Req. #10.5.2]

6.6 Audit trail files must be promptly backed up to a centralized log server or media that is difficult to alter. [SAQ Req. #10.5.3]

6.7 Audit logs for external-facing technologies (firewalls and routers) must be offloaded or copied onto a secure centralized internal log server or media. [SAQ Req. #10.5.4]

7. **Clock synchronization**

   7.1 The clocks of production environment information systems within UWM are synchronized using an external time synchronization technology such as Network Time Protocol (NTP) Server. The external time server that provides accurate, reliable, and secure time synchronization feeds to a central internal time server which further pushes to all internal production servers in the cardholder data environment. [SAQ Req. #10.4]

   7.2 The clocks on all servers in the cardholder data environment are checked on a regular basis and corrected where necessary.

8. **Log Management**
8.1 Only individuals who have a job related need can view audit trail files. No generic ids, only unique ids with specific roles with job related needs are configured to logon to the log servers. [SAQ Req. #10.5.1]

8.2 File integrity monitoring or change-detection software must be used for logs to ensure that existing log data cannot be changed without generating alerts to the Log Server Administrator/Log Reviewer. [SAQ Req. #10.5.5]

9. File Integrity Monitoring

9.1 File integrity monitoring and change detection processes must be used to monitor: [SAQ Req. #11.5(a)]
   9.1.1 System executables
   9.1.2 Application executables
   9.1.3 Configuration and parameter files
   9.1.4 Centrally stored, historical or archived, log and audit files

9.2 Alerts generated by the change detection solution are reviewed by the Log Administrator and are passed on to the relevant System Administrators for remediation. [SAQ #11.5 and #11.5.1]

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]*.