Application Development 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 2.0</td>
<td>Aug 2014</td>
<td>ControlCase</td>
<td></td>
</tr>
<tr>
<td>Draft Version 3.0</td>
<td>28-Oct-14</td>
<td>Mary Luebke</td>
<td>Document Reformatted</td>
</tr>
<tr>
<td>Final Version 3.0</td>
<td>03-Nov-14</td>
<td>Credit Card Acceptance Committee Designees</td>
<td>Document revised for UWM cardholder environment and cardholder data.</td>
</tr>
<tr>
<td>Draft Version 3.1</td>
<td>06-Aug-15</td>
<td>Credit Card Acceptance Committee Designees</td>
<td>Updated for annual review and v3.1 changes.</td>
</tr>
</tbody>
</table>

# Annual Document Review History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Reviewed By</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>03-Nov-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>09/08/2016</td>
<td>Robert Wagner</td>
<td></td>
</tr>
</tbody>
</table>
1. Purpose

The purpose of this policy is to set the requirements to be followed for secure management of system development and maintenance in the cardholder data environment at the University of Wisconsin-Milwaukee (UWM).

2. Scope

This policy will apply to all UWM applications being developed or modified in-house in the cardholder data environment. All stages of the system development life cycle are covered.

3. Policy

3.1 There must be separate development/test and production environments. [SAQ Req. #6.4.1(a)]

3.2 There must be defined segregation of duties between personnel assigned to development/test environment and personnel assigned to production environment. [SAQ Req. #6.4.2]

3.3 Production data (e.g.: live PANs) must not be used for testing and development. [SAQ Req. #6.4.3]

3.4 Test data and test accounts must be removed before a production system becomes active. [SAQ Req. #6.4.4]

3.5 Pre-production and/or custom application accounts, user IDs and/or passwords must be removed before system goes into production or is released to customers. [SAQ Req. #6.3.1]

3.6 Custom code reviews must be performed by individuals other than originating code author prior to release to production or customers in order to identify any potential coding vulnerability. [SAQ Req. #6.3.2]

3.6.1 Code reviews ensure code is developed according to secure coding guidelines. [SAQ Req. #6.3.2]

3.6.2 Appropriate corrections are implemented prior to release. [SAQ Req. #6.3.2]

3.6.3 Code-review results are reviewed and approved by management prior to release. [SAQ Req. #6.3.2]
3.7 Use of automated code review and testing tools shall be considered for proper reviews. [SAQ Req. #6.3.2]

3.8 All the resources responsible for application development, testing and code review shall be trained periodically by professionals on their specific domain related to secure coding techniques, security testing and secure code review. The training shall include the industry standard practices and guidelines. [SAQ Req. #6.3.2 and #6.5(b)]

3.9 Code reviews for custom software development, as part of the System Development Life Cycle (SDLC), can be conducted by internal personnel with required skillset and adequate professional background. [SAQ Req. #6.3.2]

3.10 Change control procedures must be followed for all custom developed system and software configuration changes. Change management procedure should include: [SAQ Req. #6.4 and #6.4.5(a)]

3.10.1 For each change there must be management sign-off by appropriate parties. [SAQ Req. #6.4.5(a) and #6.5.4.2]

3.10.2 Documentation of impact [SAQ Req. #6.4.5(a) and #6.5.4.1]

3.10.3 Operational functionality testing must be performed to verify that the change does not adversely impact the security of the system. [SAQ Req. #6.4.5(a) and #6.5.4.3(a)]

3.10.4 For custom code changes, verify that all updates are tested for compliance with following vulnerabilities at minimum before being deployed into production. [SAQ Req. #6.4.5.3(b) and #6.5]

3.10.4.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. [SAQ Req. #6.5.1]

3.10.4.2 Buffer overflows [SAQ Req. #6.5.2]

3.10.4.3 Insecure cryptographic storage [SAQ Req. #6.5.3]

3.10.4.4 Insecure communications [SAQ Req. #6.5.4]

3.10.4.5 Improper error handling [SAQ Req. #6.5.5]

3.10.4.6 Cross-site scripting (XSS) [SAQ Req. #6.5.7]

3.10.4.7 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). [SAQ Req. #6.5.8]

3.10.4.8 Cross-site request forgery (CSRF) [SAQ Req. #6.5.9]

3.10.4.9 Broken authentication and session management [SAQ Req. #6.5.10]

3.10.5 Back-out procedure must be defined for each change. [SAQ Req. #6.4.5(a) and #6.5.4.4]
3.11 All web applications must be developed based on secure coding guidelines such as the Open Web Application Security Project (OWASP) Guidelines, SANS CWE Top 25, CERT Secure Coding, etc. This is to prevent common coding vulnerabilities in software development processes. [SAQ Req. #6.5(c)]

Please refer to the Cardholder Data Information Security Policy and the Code Review Template document for information on security controls for application and common coding vulnerabilities.

3.12 All developers and testers must undergo training in secure coding techniques based on industry best practices and guidance. [SAQ Req. #6.5(b)]

3.13 All web-facing applications must be protected against known attacks: [SAQ Req. #6.6]

3.13.1 Running an application-layer firewall in front of web-facing applications.
3.13.2 Alerts generated by the application layer firewall are sent to the PCI syslog. The logs will be reviewed per the Log Review Procedure.
3.13.3 When application-layer firewall updates are available, they are applied using the Patch Management Procedure.
3.13.4

4. 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]*.