

## PROJECT CHARTER - PCI Compliance

<b>Project Name</b>	<b>PCI Compliance (Campus-Wide Charter)</b>
<b>Project Manager</b>	Bert Schnell
<b>Sponsor</b>	Don Miner
<b>Customer</b>	Controller UW Madison Cash Management
<b>Document Version and Date</b>	Version 3.2 Updated August 11, 2010

<b>Project Scope</b>	
<b>Business Need</b>	<p>University of Wisconsin - Madison accepts Credit Card for many items and services. Once the UW accepts the Credit Card we become responsible for the security of our end users Cardholder Data until destroyed or encrypted. Besides the duty we have to maintain the security of our end users Cardholder Data there are many consequences. We would need to remediate any Cardholder Data compromised which is estimated at \$204 per PAN. We will be fined by the card issuers as high as \$200,000 per occurrence. More importantly the University of Wisconsin image would be tarnished. Card Holders may become reluctant to donate or do business with the University of Wisconsin which could result in loss revenue. Similarly the card issuers are requiring we have a PCI Compliance plan and audit our systems to continue Credit Card processing.</p> <p>We can reduce the risk of compromised Card Holder Data by securing our network, hardware, applications, processes and meet PCI Compliance.</p>
<b>Project Goals</b>	<p>To design a PCI Infrastructure with Documented Processes that will assist departments implement specific policies and operating procedures surrounding their payment card-processing infrastructure. The goal is that all merchants comply with the data security standards and their requirements:</p> <p><b>PCI DSS:</b></p> <ol style="list-style-type: none"> <li>1. Build and Maintain a Secure Network             <ol style="list-style-type: none"> <li>a. Install and maintain a firewall configuration to protect data</li> <li>b. Do not use vendor supplied defaults for system passwords and other security parameters</li> </ol> </li> <li>2. Protect Cardholder Data             <ol style="list-style-type: none"> <li>a. Protect stored data</li> <li>b. Encrypt transmission of cardholder data and sensitive information across public networks</li> </ol> </li> <li>3. Maintain a Vulnerability Management Program             <ol style="list-style-type: none"> <li>a. Use and regularly update anti- virus software</li> <li>b. Develop and maintain secure systems and applications</li> </ol> </li> <li>4. Implement Strong Access Control Measures             <ol style="list-style-type: none"> <li>a. Restrict access to data by business need-to-know</li> <li>b. Assign a unique ID to each person with computer access</li> <li>c. Restrict physical access to cardholder data</li> </ol> </li> <li>5. Regularly Monitor and Test Networks             <ol style="list-style-type: none"> <li>a. Track and monitor all access to network resources and cardholder data</li> <li>b. Regularly test security systems and processes</li> </ol> </li> <li>6. Maintain an Information Security Policy             <ol style="list-style-type: none"> <li>a. Maintain a policy that addresses information security</li> </ol> </li> </ol> <p><b>PA DSS:</b></p> <ol style="list-style-type: none"> <li>1. Implementing a PA-DSS compliant payment application into a PCI DSS compliant environment.</li> <li>2. Configuring the payment application (where configuration options are provided) according to the <i>PA-DSS Implementation Guide</i> provided by the vendor.</li> <li>3. Configuring the application in a PCI DSS compliant manner.</li> <li>4. Maintaining the PCI DSS compliant status for both the environment and the application configuration.</li> </ol> <p><b>Business Processes:</b></p> <ol style="list-style-type: none"> <li>1. Segregate Duties             <ol style="list-style-type: none"> <li>a. Transactions</li> <li>b. Refunds</li> <li>c. Reconciliations</li> </ol> </li> </ol>

	<ol style="list-style-type: none"> <li>2. Segregate PC Terminals <ol style="list-style-type: none"> <li>a. General Business Activities</li> <li>b. Card processing</li> </ol> </li> <li>3. Establish Credit Card Handling Procedures</li> <li>4. Establish Data Retention Polices <ol style="list-style-type: none"> <li>a. Term</li> <li>b. Spreadsheets</li> </ol> </li> <li>5. Prohibit Transmission of CHD <ol style="list-style-type: none"> <li>a. Email</li> <li>b. FAX</li> <li>c. Text</li> <li>d. IM</li> <li>e. Campus Mail</li> </ol> </li> <li>6. Establish Storage of CHD Policy</li> <li>7. Establish Disposal of CHD Policy</li> <li>8. Mandate Notification and Approval of New Software Purchases that have PCI components</li> <li>9. SAQ's are Mandatory</li> <li>10. Annual Training of Site Managers</li> <li>11. Conduct Background Checks of Personnel</li> </ol>
<b>In Scope/Out of Scope</b>	<p>In Scope:</p> <ol style="list-style-type: none"> <li>1. Any entity depositing money into UW-Madison bank account.</li> <li>2. All UW- Madison campus merchants accepting credit card payments – point of sale operations/ mail order/ telephone order and online orders.</li> </ol> <p>Out of Scope:</p> <ol style="list-style-type: none"> <li>1. UW System schools and Colleges other than UW-Madison accepting credit card payments</li> <li>2. UW- Madison campus departments accepting other forms of payment- cash/ e-payment.</li> </ol>
<b>Project Assumptions</b>	<ol style="list-style-type: none"> <li>1. UW-Madison will have a PCI breach.</li> <li>2. PCI-CAT has the authority to negotiate with Elavon and Acquirers for our compliance.</li> <li>3. Acquirers are willing to negotiate with the UW</li> <li>4. PCI-CAT has the authority to establish Policies and Procedures for SToP CHD.</li> <li>5. PCI-CAT has authority to utilize resources.</li> <li>6. PCI-CAT will access external resources when required.</li> <li>7. Continuity of Operations</li> <li>8. PCI <u>will not</u> improve System Availability.</li> <li>9. PCI Compliance Systems Design Requirements: <ol style="list-style-type: none"> <li>a. Availability is Low to Medium</li> <li>b. Confidentiality is High</li> <li>c. Auditability is High</li> </ol> </li> </ol>
<b>Project Constraints</b>	<ol style="list-style-type: none"> <li>1. Missed initial PCI deadline.</li> <li>2. Limited staff resources</li> <li>3. PCI Rules are evolving</li> <li>4. Merchant environment is ever changing</li> </ol>
<b>Project Deliverables</b>	<ol style="list-style-type: none"> <li>1. UW-Madison will provide an attestation of PCI Compliance to our Acquirers.</li> <li>2. Merchant Analysis</li> <li>3. Document Business Processes</li> <li>4. Develop Merchant ID Tracking Application</li> <li>5. Develop Policies and Procedures</li> <li>6. Develop Data Center &amp; Infrastructure</li> <li>7. Develop Training</li> <li>8. PCI Implementation to each Site</li> </ol>
<b>UW Risks</b>	<ol style="list-style-type: none"> <li>1. Brand Damage</li> <li>2. Fines from Acquirers</li> <li>3. Remediation Costs</li> </ol>
<b>Benefits</b>	<ol style="list-style-type: none"> <li>1. Preserve the Brand</li> <li>2. Mitigate Fines from Acquirers</li> <li>3. Reduce Remediation Costs</li> <li>4. Continue to Process Credit Cards</li> </ol>

<b>High-Level Milestones</b>		
<ol style="list-style-type: none"> <li>1. Merchant Analysis</li> <li>2. Document Business Processes</li> <li>3. Develop Merchant ID Tracking Application</li> <li>4. Develop Policies and Procedures</li> <li>5. Develop Data Center &amp; Infrastructure</li> <li>6. Develop Training</li> <li>7. PCI Implementation to each Site</li> </ol>		
<b>Project Team, Roles, and Responsibilities</b>		
<b>Name/Division</b>	<b>Roles</b>	<b>Responsibilities</b>
Joanne Berg, CIO & Vice Provost for Information Technology	Sponsor	Leadership & Vision
Darrell Bazzell, Vice Chancellor for Administration	Sponsor	Leadership & Vision
Don Miner, Assistant Vice Chancellor of Business Services	Middle Manager	Product Acceptance
Jim Lowe, CISO, Office of Campus Information Security (OCIS)	Middle Manager	Product Acceptance
Al Benzschawel, Controller	Middle Manager	Product Acceptance
Sharon Hughes, Supervisor of Cash Management	Core Team	Business Expertise
Padmini Prashanth, Cash Management, CASHNet Interface	Core Team	Business Expertise
Janet Hamm, Cash Management, Elavon Interface	Core Team	Business Expertise
Jeff Savoy, OCIS	Core Team	IT Infrastructure Expertise
Tom Callaci, OCIS	Core Team	IT Security
Carl Hubbard, Purchasing Services	Core Team	Purchasing Expertise
Bert Schnell, DoIT	Project Manager	

<b>Communications Strategy</b>	
<b>Internal</b>	<b>Team</b> <ol style="list-style-type: none"> <li>1. Weekly Meetings</li> <li>2. Email progress of Tasks</li> <li>3. My WebSpace</li> </ol> <b>Stakeholders</b> <ol style="list-style-type: none"> <li>1. Identify DBR &amp; Site Managers</li> <li>2. Conduct Initial Education</li> <li>3. Periodic Notifications of Milestones</li> </ol>
<b>External</b>	<b>Elavon</b> <ol style="list-style-type: none"> <li>1. Negotiate Level of Compliance</li> <li>2. Notify Project Status</li> <li>3. Notify any Breaches</li> </ol> <b>Public</b> <ol style="list-style-type: none"> <li>1. Notify any Breaches</li> </ol>
<b>Third Party</b>	<b>New Software Providers</b> <ol style="list-style-type: none"> <li>1. PCI Compliance</li> </ol>

<b>Term, Abbreviation or Acronym</b>	<b>Definition</b>
<b>CHD</b>	<b>Card Holder Data</b>
<b>DBR</b>	<b>Division Business Representative</b>
<b>DSS</b>	<b>Data Security Standard</b>
<b>Hashing</b>	<b>Render cardholder data unreadable</b>
<b>ISA</b>	<b>Internal Security Assessor</b>
<b>Masking</b>	<b>Method of concealing a segment of data displayed</b>
<b>PAN</b>	<b>Primary Account Number</b>
<b>PCI</b>	<b>Payment Card Industry</b>
<b>SToP</b>	<b>Store, Transmit or Process</b>
<b>QSA</b>	<b>Qualified Security Assessor</b>
<b>SAQ</b>	<b>Self-Assessment Questionnaire</b>
<b>Site</b>	<b>Business Operation</b>
<b>ISA</b>	<b>Internal Security Assessor</b>

See link below for additional definitions: [pci\\_dss\\_glossary.pdf](#)