PAYMENT CARD INDUSTRY COMPLIANCE TEAM (PCI CT) CHARTER

Project Name	**PCI Compliance Team (Campus-Wide Charter)**
Executive Sponsor	Data Governance Steering Committee
Business Sponsor	Martha Kerner / Dan Langer
IT Sponsor	Jason Fishbain / Bob Turner
Document Version and Date	Version 5 – Updated October 4, 2015

Team Scope	
Background	The University of Wisconsin – Madison processes over $100 million dollars in credit card transactions per year. In fiscal year 2014 this includes 2.82 million transactions from 215 merchant accounts. The University is contractually responsible for protecting the credit card data used to process these transactions per the guidance provided by the PCI Data Security Standard (PCI-DSS). There were numerous publically scrutinized breaches that occurred in 2014 including Target, Neiman Marcus, Michaels, Dairy Queen, UPS, Goodwill, and Home Depot. This is an indication that these breaches can happen. A credit card breach may result in fines starting at $200,000. However, the actual costs of a credit card breach are estimated around $204 per credit card. More importantly, the UW-Madison's image would be tarnished. This could result in fewer donors willing to support the University or business partners willing to acquire University resources. UW-Madison can reduce the risk of compromised Card Holder Data by securing the network, hardware, applications, processes and meeting PCI Compliance requirements.
Team Goals	There are five primary goals of the PCI CT. 1. Establish a risk-based approach to promote and require all UW-Madison merchants to achieve compliance with the PCI Data Security Standards. In this regard, serve as the first point of contact for merchant account establishment. 2. Support the PCI Network Infrastructure and Applications that conduct business on campus. This essential primary goal of PCI Compliance. Compliance cannot be maintained without maintenance, updating, and risk analysis of this network. 3. Leverage a centralized service to support PCI Compliance. The PCI Compliance Team completes several of these compliance requirements for the entire campus, including but not limited to, network infrastructure and equipment, change control, physical security of the data center, training, policy, and risk analysis. 4. Monitor PCI-DSS requirements and cyber security trends. The PCI CT provides technical analysis of trends related to credit card processing. 5. Review and monitor individual campus merchants to ensure compliance with the PCI-DSS requirements.
Team Deliverables	1. Provide centralized training for campus annually and as new merchant accounts are established. 2. Complete PCI related compliance reporting requirements to the bank annually or as needed. 3. Provide and support technical infrastructure to meet PCI compliance

	requirements. 4. Maintain and update policy requirements for campus annually. 5. Review and monitor PCI compliance requirements. 6. Research trends in the credit card payment process. This may include chip and pin technology, mobile payments and other payment technology. 7. Annually provide metrics of these deliverables to the Data Stewardship Council.
Team Authority	The PCI CT has the authority to ensure campus merchants are complying with PCI requirements. PCI CT has the authority to establish and discontinue merchant activities based on the PCI compliance of credit card processing practices. The authority of the PCI CT covers PCI compliance only, and does not include assessing business needs or setting direction regarding the extent of credit card usage on campus.
In Scope/Out of Scope	In Scope: 1. All UW-Madison campus merchants accepting credit card payments that deposit money to a UW-Madison bank account. 2. Any entity that stores credit card data on campus in a merchant capacity. 3. PCI CT enforces that all merchants have an appropriate service provider. Out of Scope: 1. UW System schools and Colleges other than UW-Madison accepting credit card payments. 2. UW- Madison campus departments accepting other forms of payment- cash/ e-payment. 3. Any external fundraising arms of the University.

PCI CT CORE TEAM MEMBERS	
Name/Division	**Title**
Jeff Endres	IT Security
Open	Risk Management
Sharon Hughes	Cash Management Supervisor
Mike Halton	Cash Management, Accountant
Janet Hamm	Cash Management, Accountant
Dan Langer	Controller
Andrew Norman	Legal Affairs
Hartley Murray	Purchasing
Bruce Riley	Purchasing
Jeff Savoy	Information Security Officer

Communication Partners	
Internal	Data Governance Steering Committee
External	Elavon US Bank

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

ISA	**Internal Security Assessor**

pci_dss_glossary.pdf