

UW-Madison Payment Card Industry Compliance Structure

What is PCI compliance for a credit card accepting merchant? PCI compliance means that a merchant accepting credit or debit cards is operating in a way that protects the confidential information (card number, expiration date, name of cardholder and security code) from being released to anyone other than the acquirer of the transactions going into the credit card processing network. The standards are set by the PCI Standards Council established by the major card brands.

1. Computer applications used to accept and process credit cards must be certified to be PA-DSS compliant by the PCI Security Standards Council (certifications appear on their website with version numbers of computer applications of vendors which are deemed compliant).
2. The environment in which that application runs; people, hardware and networks must be deemed PCIDSS compliant as documented by completion of one of 4 Self-Assessment Questionnaires (A, B, C or D) published by the Standards Council.
3. The transaction acquirer (Elavon, a subsidiary of US Bank is the acquirer for 99% of our charge card business) reviews the situation and provides a 1-4 (bad to good) PCI ranking for the “merchant” (merchant can be a collection of merchant IDs). These rankings determine how frequently certain follow-up procedures are required, such as obtaining a report from a Qualified Security Assessor. If there is a data breach a merchant is moved immediately to level 1. Level 1 compliance requirements are costly.

In the event of a compromise, the credit card companies evaluate your compliance and levy fines until such time that you are compliant. Visa fines are \$50k first compromise and go up, MasterCard \$25k per day for each day of non compliance, American Express, \$50k first occurrence of non-compliance, Discover \$100k max per violation.

UW-Madison’s governance strategy is outlined on the back side of this page. The model follows our normal accountability model of school/college/administrative unit’s Dean or Director being the responsibility point for activities happening under their watch through their Divisional Business Representative. A campus-level PCI Compliance Assistance Team (PCICAT) is available to assist and if necessary enforce certain changes if a merchant is to be allowed to continue operations.

Here are some key parts of our operational plan:

1. Every one of our 250+ merchants will be required to fill out a self assessment questionnaire which will be maintained centrally and renewed periodically. We are currently in the process of developing a comprehensive inventory of our merchants, what they sell and how they operate.
2. We have hired a consultant to put our compliance plan together and help us negotiate our level of compliance with Elavon.
3. We are developing a PCI compliant server platform for use with applications which require a server to store or process card numbers. We are identifying a specific very secure band of the 21st Century Network which will be used to communicate between those servers and points of sale.
4. We have contracted with CashNet (now part of Higher One) to manage the card processing originating from our 100+ web storefronts. CashNet’s service has been certified PCI compliant.
5. We will be developing standardized training for site managers and operators.

The most important thing any of you or your merchants can do is talk with PCI CAT before making changes in card handling processes, before getting into the credit card business, or to ask for a review of current procedures.

01-10-11
UW-Madison Payment Card Industry Compliance Structure

UW-Madison PCI Compliance Project Structure	
Sponsors	Darrell Bazzell, Vice Chancellor for Administration Chief Information Officer
Middle Managers	Don Miner, Assistant Vice Chancellor for Business Services Jim Lowe, CISO, Office of Campus Information Security (OCIS) Al Benzschawel, Controller
Core Team	Sharon Hughes, Supervisor of Cash Management Mike Halton, Cash Management, PCI help desk and training coordinator, Cashnet interface (PCI-Help@bussvc.wisc.edu) Janet Hamm, Cash Management, Elavon and Cashnet interface (CashNet-Help@bussvc.wisc.edu) Jeff Savoy, OCIS Tom Callaci, OCIS Carl Hubbard, Purchasing Services Bert Schnell, Project Manager (DoIT)
Divisional Business Representative (DBR)	Responsible for all merchants in their division. Will sign the attestation for PCI compliance for their division.
Site Managers	Those who are responsible for one or more merchant ID numbers
Operators	Those who work within the site manager's unit and process credit card transactions

1. The PCI Site Manager/operator concept is very similar to what we do to manager 2500 purchasing cards. Cardholders are the responsibility of site managers with the average manager handling 12 cards. Our communication of policy and procedure is to the Divisional Business Manager and the site managers who communicate with their cardholders. Separate training is provided to site managers and to card holders.
2. The Divisional Business Rep is responsible for the site managers in their division (school, college, admin unit) and would be responsible for annual attestation of PCI Compliance.
3. The sponsors are generally accountable to the outside world for our compliance with PCI and provide the project with resources to help the site managers and operators comply. They also approve institutional policies.
4. The middle managers provide the central team with resources and enforcement assistance. They also create consensus on institutional policies.

01-10-11

UW-Madison Payment Card Industry Compliance Structure

5. The core team members work through the Divisional Business Representative directly with merchants and services providers. They should refer issues to the middle managers if they are having difficulty with any of the PCI Site Managers or operators.