

UW-Green Bay Guidelines for Departments and Employees

Handling Payment Card Industry (PCI) Transactions

(Version 1.03, 3/6/2009)

To enhance the security and safekeeping of payment card information, the following guidelines have been developed. This information should be shared and reviewed with employees when they are initially hired and on an annual basis.

- 1) Cardholder data (name, address, personal account number, expiration date, service code, PIN verification value and/or verification code or value) information needs to be protected at all times. The three digit CID/CVV 2/CVC 2 card verification code and/or PIN verification value must not be retained on paper or electronically. Only specific authorized employees, on a business need to know basis, should have access to the information. Any paper records (i.e., forms, faxes, etc.) that contain this information must be kept from the access and sight of unauthorized persons at all times. All paper records that contain this information must be physically secured (locked in desk, file cabinet, office, or storage room) when not in use by an authorized employee.
- 2) Any paper forms that show only the last four digits of the card holder data should be retained for a minimum of the current fiscal year, plus three additional years. As soon as the cardholder data is no longer needed, it should be blacked out on the original form. Merchant copies of credit card receipts must be retained for ninety days after the event. After that point, they should be securely destroyed. All forms that have cardholder data should be secured in a file cabinet or room that only specifically authorized persons can access. All storage boxes containing credit card information should be clearly marked as confidential. All forms and credit card receipts containing cardholder data must be securely destroyed (cross cut shredded or secure recycling) when they are no longer needed.
- 3) Electronic or paper records containing cardholder data should never leave the campus unless their continuous, physical security can be guaranteed and you have the explicit permission of your supervisor.
- 4) Cardholder data should never be copied to a laptop, storage device, personal digital assistant (PDA), smartphone, or other removable media without the explicit permission of the employee's supervisor.

- 5) Credit card information can be accepted by telephone, mail, fax, or in person only. Cardholder information must never be received or sent via unencrypted methods including email, instant messaging, chat, or unsecured web page technologies.
- 6) PCI industry rules require that cardholder data be secure and encrypted when it is stored electronically on campus workstations, servers, or with outside providers. Departments should not retain cardholder data in electronic form (i.e., entered into spreadsheets, databases, or application package) if at all possible. Unless the application package or database is specifically setup to encrypt this information, the data is probably not encrypted and we are not in compliance with PCI industry rules. It is safer for the University and the cardholder that we not store their information, especially if we cannot store the data in an encrypted form. This does imply that you will have to contact the user to get card information to process some refunds. If you need to electronically store cardholder data, you should work with the campus IT Security Officer to identify options to provide proper security of the information.
- 7) Any terminals, cash registers, or other devices that print customer or merchant receipts should only print the last four digits of the personal account number. Receipts must not include the expiration date for the card.
- 8) If your application uses the campus network to handle or store transactions, you need to work with the campus IT Security Officer to ensure the data is handled securely.
- 9) All forms used by customers to submit cardholder data should be designed so that the cardholder information is not in clear view when mailed.
- 10) Each person should be assigned a unique username and password for accessing cardholder data that is stored electronically.
- 11) All employees authorized to handle cardholder information should review the campus information security policy and this document when initially hired and on an annual basis. The policy is located on the campus web server.
- 12) If an employee is informed of, or suspects that a breach of PCI data may have occurred, they must immediately report this to their supervisor and the campus IT Security Officer for investigation.

If you have any questions in regards to these guidelines, please discuss them with your supervisor or contact the campus IT Security Officer for clarification.