

SUBJECT: Cardholder Information Security Procedures	Effective Date: 07-24-08	Policy Number: 3-206.3	
	Supersedes: 3-206.2	Page 1	Of 4
	Responsible Authority: University Controller		

ACCOUNTABILITY/APPLICABILITY:

This policy applies to all individuals who have access to credit card information in any form at any merchant location of the University of Central Florida.

POLICY STATEMENT:

All university employees and third parties that have access to hold cardholder data will hold the data in confidence at all times and will disclose cardholder information only for a required business purpose.

DEFINITIONS:

Audit logs. A registry that shows the identifier, date, and time that stored data is accessed.

Cardholder Information Security Program (CISP). The payment card industry's security standards for protecting credit card information.

Cross shredding. The process of using a shredder to cut paper both vertically and horizontally to more completely destroy documents.

Degaussing. The process of completely removing information from electronic media so that it can no longer be retrieved.

Employees. Individuals acting on behalf of the university in processing, storing, and retrieving credit card data. This includes individuals in the following classifications: faculty, University Support Personnel (USPS), Administrative and Professional (A&P), Other Personal Services (OPS), students, and volunteers.

Encrypted or truncated. Data converted to a code or shortened for security purposes.

Merchant location. Any university business unit that accepts credit cards as a form of legal tender, including retail and Web-based operations.

Payment card industry. The association of credit card providers. The university accepts the following credit cards: VISA, MasterCard, American Express, Diners Club, and Discover. In addition, the university accepts debit cards and electronic checks.

Self-assessment. The CISP-required annual review of procedures and processes to ensure compliance with current security standards.

Third party. Companies or individuals that have a relationship with the university to supply goods and/or services. For purposes of this policy, the third party must have direct or indirect access to cardholder information.

Validation code. The unique three- and four-digit codes printed on the backs of credit cards that merchants may request as proof that a credit card is in the possession of the individual making or completing a transaction.

PROCEDURES:

UCF conforms to certain standards to protect credit card information held and/or used at the university. Responsibilities and requirements for the following persons and units are listed below.

1. Employees with access to credit card information must:
 - a. have a background check by Human Resources before being granted access to cardholder information. Employees with an inappropriate background will not be permitted to have access to cardholder information.
 - b. attend a credit card information security training session or a security awareness program offered by UCF.
 - c. sign the Credit Card Security Ethics Certification (F&A Form 41-915) to document his or her understanding of and willingness to comply with all university credit card policies and procedures. This certification will be maintained in the employee's personnel file.
 - d. attend an annual UCF credit card information security training session or a security awareness program.

2. Merchant locations must:
 - a. provide each employee with a unique password that expires after sixty days to access credit card data (other than single transaction processing).
 - b. protect cardholder information so that no more than the first six and the last four digits of the credit card number are displayed or printed.
 - c. store only credit card information that is critical to business name, account number, and expiration date.
 - d. store only cardholder data that is encrypted or truncated.
 - e. never store the three- or four-digit validation code in any form.
 - f. not release credit card information in any form unless there is a legitimate business purpose and then only after the request for information is reviewed and approved by the unit's management.

3-206.3 Cardholder Information Security Procedures 2

- g. provide secure access of the cardholder data at all times if wireless connections are used, and test controls, limitations, network connections, and restrictions annually to stop unauthorized access attempts.
- h. use a wireless analyzer at least quarterly to identify all wireless devices in use for their compliance with payment card industry data security standards.
- i. store and secure cardholder data in locked containers identified and classified as confidential in secured areas with limited access. Examples include electronic data, customer receipts, merchant duplicate receipts, and reports.
- j. perform an annual review of critical data storage to ensure that all security requirements are met.
- k. provide all third party vendors with a copy of university credit card policies.
- l. provide all third party vendors with a unique user ID that includes a password that expires every sixty days.
- m. give third party vendors access to credit card data only after a formal contract is signed that outlines the security requirements and requires adherence to the payment card industry security requirements.
- n. not store cardholder information on laptop, notebook, or mobile computing devices at any time.
- o. deploy anti-virus software on all systems commonly affected by viruses and ensure that the programs are capable of detecting, removing, and protecting from other forms of malicious software, including spyware and adware.
- p. annually review, update, and post official written policies and procedures regarding credit card information security.
- q. use Bank of America merchant services' for all credit card processing.
- r. ensure that the PC(s) used to connect to the Bank of America Payment Collection Gateway:
 - i. complies with computer security standards outlined at www.infosec.ucf.edu.
 - ii. blocks outside Internet access except to the Payment Collection Gateway.
 - iii. prohibits the use of e-mail to avoid security breaches.
 - iv. has its security level zone set to 'high' for the Internet.
 - v. requires each user to have unique sign-on identification.
- s. complete an annual Payment Card Industry DSS (Data Security Standard) Self-Assessment Questionnaire(s) and correct all identified weaknesses as soon as possible but no later than 90 days after weaknesses are identified, or face suspension.
- t. merchant locations must dispose of cardholder data after one year by overwriting or degaussing magnetic media or cross-shredding paper.

3. Finance & Accounting and Computer Services must:

- a. annually review, update, and post official university-wide written policies and procedures regarding credit card information security.
- b. perform an annual self-assessment in partnership with an independent compliance partner that is certified by the cardholder industry.

3-206.3 Cardholder Information Security Procedures 3

- c. implement and maintain policies and procedures to monitor merchant locations for CISP compliance.
- d. provide policy and procedure training to new merchant administrators prior to providing merchant numbers to new entities.
- e. review access logs daily for all system components.
- f. deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content file and perform critical file comparisons daily.
- g. provide firewalls and perform penetration testing at least once a year and after any significant infrastructure upgrade or when a sub-network or web server is added to the environment.
- h. maintain audit trail history in hard copy for at least one year and for at least three months online.
- i. conduct a quarterly review of network or host-based firewall or router rule sets.
- j. Monitor merchant locations annual PCI DSS self-assessment questionnaires for compliance and suspend non-compliant merchant accounts when identified weaknesses are not corrected in a reasonable period of time.

4. Loss or Theft

When a university employee suspects the loss or theft of any materials containing cardholder data, it is vitally important to immediately notify the supervisor and the director of the merchant location. Upon confirmation of the cyber-loss or theft, the director of the merchant location must follow the Security Incident Response Plan and implement the procedures for security breach. The director of the merchant location must also notify the Operations Office of Computer Services & Telecommunications or the CS&T Service Desk. If loss of cardholder information is due to a physical break-in, the director of the merchant location must immediately contact the UCF Police Department.

RELATED INFORMATION:

Security Incident Response Plan and Procedures for Security Breach:

http://www.infosec.ucf.edu/Security_Incident_Response_Plan_HL.pdf

http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html?it=12|/merchants/risk_management/cisp.html|If%20Compromised

CONTACTS:

Finance and Accounting Merchant Services:

http://www.fa.ucf.edu/Auxiliary/Merchant_Services/Merchant_Services.cfm

Operations Center, Computer Services & Telecommunications (407) 823-2908.

CS&T Service Desk (407-823-5117) or servicedesk@mail.ucf.edu

INITIATING AUTHORITY: Vice President for Administration and Finance

3-206.3 Cardholder Information Security Procedures 4

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 3-206.3

Initiating Authority: Will I. Mamba Date: 2/26/09

Policies and Procedures
Review Committee Chair: John P. Luce Date: 2-26-09

President or Designee: John C. Hill Date: 2/27/09