Office of Compliance and Ethics
UNIVERSITY of WEST FLORIDA

PCI DSS Compliance Training for Employees Exposed to Customer Cardholder Data

Introduction - Customer credit card numbers are extremely sensitive information and should be kept secure and safeguarded at all times. The University is required to comply with the Payment Card Industry Data Security Standards (PCI DSS), and has adopted strict procedures to ensure compliance. Employees whose duties may expose them to customer credit card data must receive official training before assuming those duties. ***Employees that have not received official training should immediately contact the Office of Compliance and Ethics if they receive, or are exposed to any documents or electronic files containing cardholder information.***

Credit Card Webpage – The Office of Compliance and Ethics has established a webpage to consolidate the rules, regulations, procedures, forms and other information related to the security of customer cardholder data. Employees that work with cardholder data should review and be familiar with the information on this webpage.

Payment Card Industry (PCI) Security Standards Council – Several of the major credit card companies founded a joint council to provide standardization of the rules and requirements between the different brands. The council has issued sets of standards applicable to all vendors who use any of the credit card brands for the collection of revenues.

Payment Card Industry Data Security Standards (PCI DSS) – Standards related to the security of customer cardholder data. The standards include twelve requirements, each of which has multiple sub-requirements. The twelve requirements are grouped into the following six categories:

1. *Build and Maintain a Secure Network*
2. *Protect Cardholder Data*
3. *Maintain a Vulnerability Management Program*
4. *Implement Strong Access Control Measures*
5. *Regularly Monitor and Test Networks*
6. *Maintain an Information Security Policy*

Cardholder Data – Consists of the full credit/ debit card number, also known as the Primary Account Number (PAN) plus any of the following:

- *Cardholder name*

- *Expiration date*
- *Service code*

The last four digits of the credit card number may be maintained for reference and do not constitute cardholder data. Customer receipts should not show more than the last four digits of the credit card number. Computer systems and software used to process credit card transactions should not display more than the last four digits of the credit card number.

The University does not permit the storage of the codes found on the magnetic stripe, or the card validation code (three-digit code on back of credit card or four-digit code on front of American Express card).

All employees that have access to cardholder data must keep this information in the strictest confidence, and protect it from unauthorized access or disclosure. Access to this information is on a need-to-know basis only.

Electronic Credit Card Records - Information Technology Services (ITS) and the Controller's Office must review and approve the use of any hardware, software, electronic system, or external entity used to process credit card transactions. Additional guidelines follow:

- *All outside vendors that process or have access to UWF customer cardholder data must be PCI compliant*
- *Cardholder data should never be stored in any electronic format*
- *Cardholder data should never be included in email or other electronic messages*
- *Employees should not use their regular work computer for processing credit card transactions*

Paper Credit Card Records – Procedures related to the security of paper records containing cardholder data are available on the Credit Card page of the Compliance and Ethics website. General guidelines for these paper documents follow:

- *Anyone working with documents that contain credit card numbers should review the security procedures on the website referenced above*
- *Documents must be protected, stored securely, inventoried, and disposed of securely*
- *Procedures allow the elimination of credit card numbers from certain paper documents These procedures are located on the Credit Card page and should be followed precisely*

Authorization to Accept Credit Cards – All credit card collection activities must be approved in advance by the University Controller. If your department wishes to begin a new collection activity, you should submit a Request for Authorization to Accept Credit Card Transactions form prior to beginning that activity.

If you plan to modify an existing approved collection activity, please contact the Office of Compliance and Ethics to discuss the planned modifications. Significant modifications may pose new security issues and will require re-evaluation and approval. Significant modifications include, but are not limited to the following:

- *Using new/different equipment to process credit card transactions*
- *Changing software used to process credit card transactions*
- *Changing location of collection/processing area*
- *Changing outside vendors for credit card processing or significant changes in the processing procedures*

Questions/ Concerns:

Matt Packard, CCEP

Chief Compliance Officer

850.857.6070 | mpackard@uwf.edu

Reviewed September, 2018