The University of Florida Credit Card Standards

1. Introduction

As a convenience to University of Florida customers, UF units and departments may accept credit and debit cards for payments, or may outsource payment card processing to approved third-party service providers.

Currently accepted payment card brands are:

- VISA
- MasterCard
- Discover
- UnionPay (under certain conditions; please check with Payment Card Operations)
- American Express
- Debit cards with a VISA or MasterCard logo

This document and additional supporting documents represent the University of Florida's Directives and Procedures to protect our customers' personal financial information. Failure to protect such information may result in financial loss for customers, suspension of credit card processing privileges, and fines

imposed on credit card merchants and damage to the university's reputation.
These directives apply to all types of credit card activity (storage, processing and transmission of card information), including transactions processed face-to-face, over the phone, via fax, mail or the Internet (e-Commerce). Furthermore, this document provides guidance to maximize compliance with the Payment Card Industry (PCI) Data Security Standards (DSS).

1.1. UF Payment Card Operations

Payment Card Operations, a unit within UF's Treasury Management, coordinates all endeavors related to payment cards including, but not limited to, applications to create merchant accounts or to make changes to an existing account. Contact Payment Card Operations at 352-392-9057 for more information.

Any activity involving the acceptance of payments for products or services by means of credit and/or debit cards requires the approval of the University Controller's Office.

1.2. Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a mandated set of security standards agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security related standards were developed to secure all payment card information from unauthorized access and apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Further details about the PCI DSS can be found at the PCI Security Standards Council website (https://www.pcisecuritystandards.org)

In order to accept credit card payments, the University of Florida must prove and maintain compliance with the Payment Card Industry Data Security Standards. For that purpose, all merchant locations or units that store, process, or transmit cardholder data must perform an annual self-assessment in partnership with Payment Card Operations. There are multiple versions of Self-Assessment Questionnaires (SAQ) to cover various credit card processing scenarios.

2. Processes and Best Practice to Ensure Payment Card Data Security

Departments must document their processes by means of procedures that are available for periodic review, and placed in immediate proximity of the workstation/credit card terminal. These procedures must include the following components that are to be maintained on an ongoing basis.

2.1. Processing and Collection

2.1.1.	Collected cardholder data are restricted only to those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access and review the list monthly to ensure that the list reflects the most current access needed and granted.
2.1.2.	All equipment used to collect data is secured against unauthorized use or tampering in accordance with the PCI Data Security Standard.
2.1.3.	Email, text messaging, and chat should not be used to transmit payment card or personal payment information, nor should it be accepted for processing as a method to supply such information. In the event that it does occur, disposal of such payment card information is critical. If payment card data is received in an email then:
	• The email should be replied to immediately by means of a separate message stating that "The University of Florida does not accept payment card data via email as it is not a secure method of transmitting cardholder data." Do NOT include in your response any of the payment card information that was provided in the original message (CC number, expiration date, CVV code, etc.)
	• The received email will be securely destroyed as per Section 2.2.6
2.1.4.	Fax machines used to transmit payment card information to a merchant department shall be

	standalone machines with appropriate physical security; receipt or transmission of payment card data using a multi-function facsimile is not permitted.
2.1.5.	Segregation of duties is a must. Establish appropriate segregation of duties between personnel handling credit card processing, processing of refunds, and the reconciliation function.
2.1.6.	If transmitting transactions using a 'swiping' terminal or InternetSecure, settle the transactions daily before 9:30pm. This settlement process is called 'batching out'. Daily settlement of transactions will lower your merchant fees.
2.1.7.	The daily settlements have to be entered as departmental deposits into MyUFL (PeopleSoft) within one business day after settlement, if a credit card swiping machine or InternetSecure is used to process transactions.

2.2. Storage and Destruction

2.2.1.	Any type of cardholder data storage requires the prior approval of Payment Card Operations. The data needs to be protected against unauthorized access. Only the following data elements may be retained: • Cardholder Name • Primary Account Number (PAN) • Expiration Date • Service Code Cardholder data needs to be encrypted or truncated. Render PAN, at minimum, unreadable anywhere it is stored.
2.2.2.	Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or any files containing cardholder data.
2.2.3.	No database, electronic file, or other electronic repository of cardholder data is allowed.
2.2.4.	Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.
2.2.5.	Cardholder data should not be retained any longer than a documented business need; after which, it must be deleted or destroyed immediately following the required retention period. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept beyond the record retention requirements.
2.2.6.	The only acceptable destruction methods are: cross-cut shredding, incineration, and pulping so that cardholder data cannot be reconstructed.
2.2.7.	Purchasing Card data shall be protected in a similar manner and institute the above components, particularly as it relates to storage and disposal of cardholder data.
2.2.8.	It is not allowed to store the three digit card verification code on the back of a card (or four digits on the front), or PIN after authorization of a transaction.
2.2.9.	Must mask retained primary account numbers when displayed. The last four digits are the maximum number of digits to be displayed

2.3. Quarterly Processes

2.3.1.	Policies and procedures include a programmatic (automatic or manual) process to remove, at least on a quarterly basis, stored cardholder data that exceeds requirements defined in the data retention policy.
2.3.2.	Must change user passwords at least every 90 days
2.3.3.	Certain payment card processing implementations require the running of internal and external network vulnerability scans. Please contact Payment Card Operations for further details.

2.4. Annual Processes

2.4.1.	Test Incident Response Plan
2.4.2.	Staff security awareness training (incl. on new hires) The current annual training consists of two online training classes accessible in myUFL under 'My Self Service' (Training and Development). All workforce members defined as employees,

	students or volunteers, who work with (process, store, transmit) credit or debit cards are required to successfully complete **one of the two** PCI trainings initially before beginning work with payment cards and annually thereafter: **Training class TRM100** –required if the workforce member manages an area that works with or processes credit or debit cards. Manager is defined as someone who provides feedback, approves vacation and time worked, and completes performance reviews of other UF employees. **Training class TRM 150** –required for all non-supervisory, frontline employees that work with or process credit or debit cards. This includes operating swiping machine(s), or other POS systems, or staff whose unit has outsourced payment card processing to third party vendors.
2.4.3.	Staff acknowledgment of policy/procedure (incl. on new hires) Require personnel to acknowledge at least annually that they have read and understood the company's security policy and procedures. Must sign the Credit Card Security Ethics Certification (FA-TM-CCETHICS) to document annually his/her understanding of and willingness to comply with all university credit card security policies, directives and procedures as well as the PCI DSS. - This certification will be maintained in the merchant's file with Treasury Management and should be submitted to Payment Card Operations with Treasury Management, located at S-113 Criser Hall, during establishment of a new merchant location, the hiring of a new employee and/or on request. The merchant meanwhile also keeps a copy of this document on file.
2.4.4.	Merchant manager completes the following tasks and submits documents to Payment Card Operations: • Employee training validation • Review the departmental payment card procedure and update as needed • Monitor and report on PCI status of 3rd-party service providers • Completed Self-assessment Questionnaire
2.4.5.	Must verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment. Note: The UF Office of Information Security and Compliance has the authority to perform such risk assessments.

3. Credit Card Terminals (Swiping Machines):

3.1. Setting up Credit Card Terminal Account

For UF departments/units, who intend to process their credit card transactions face-to-face or in a MO/TO (Mail Order/Telephone Order) environment, by means of a credit card swiping machine: Complete and submit the following documentation to Treasury Management, Payment Card Operations, S-113 Criser Hall, PO Box 114050:

- Request for Merchant ID (see 7. Resources – Forms)
- Completion of training requirement. See 2.4.2.
- Submit Ethics Certification for each relevant staff member (FA-TM-CCETHICS). See 2.4.3.

Upon the approval from the Controller's Office Payment Card Operations will forward pertinent information to American Express as well as our credit card processor, Elavon, Inc., to set up the merchant, issue a merchant ID number, and ship a terminal to Treasury Management, where the device is logged and prepared for pick up by the merchant. The merchant/UF department will be billed directly for all equipment cost. Please contact Payment Card Operations for current pricing and available models.

3.2. Prerequisites to Apply for a Credit Card Terminal

A dedicated analog phone line is preferred; VoIP lines are acceptable, but are subject to more PCI DSS related controls.

The merchant's administrative staff need to have completed the following HR classes to obtain the security role for entering daily settlements into PeopleSoft:

PST021 - "Making Deposits in myUFL"

PST956 - "Online Journal Entry 9.1"

TRM200 - "Explaining UF Cash/Check controls"
Deposits in PeopleSoft need to be created within 24 hours of settlement. The Department Security Administrator (DSA) needs to request the security role "UF_ AR_Cashier" upon completion of the staff member's training classes.

The process to establish a new merchant location takes approximately 2 - 3 weeks.

3.3. Merchant Fees for Credit Card Terminals

The fees charged by the credit card companies and issuers are based on a variety of factors including the type of card the customer uses, and whether the transaction is swiped/inserted, or keyed in to the terminal. To obtain the lowest rate the merchant should do the following:

- Settle the terminal transactions daily. This is also called batching out
- Swipe or insert the credit cards versus keying credit card information

The price range for credit card terminals currently varies between $230 and $895. The University of Florida is using exclusively EMV enabled terminals that accommodate the usage of chip enabled payment cards (EMV). Departments are responsible for any repair cost after the one year warranty period.

Current charges are subject to change when new Interchange Rates are published in April and October of each year. The fees include, but may not be limited to, an Interchange fee charged by the issuing bank, an assessment fee charged by Visa, MasterCard and Discover, and a transaction fee charged by the credit card processor to process the transactions and provide statements. American Express transaction fees are contractually fixed (ask Payment Card Operations for current fee).

Treasury Management will charge your department/merchant based on the monthly statement received from American Express and the credit card processor.

In addition, departments are responsible for Florida Sales and Use Tax if applicable. Questions on the applicability of Sales and Use Taxes, and related reporting requirements should be addressed to University Tax Services, in the Finance and Accounting Division (Contact: 352-392-1231, or taxhelp@admin.ufl.edu).

4. E-Commerce:

4.1. Setting up an Internet-related E-Commerce Account

For UF departments/units who intend to process their credit card transactions via the Internet by means of e-Commerce:

- Contact Payment Card Operations to discuss your needs to select a University and PCI approved service provider:
- Service Providers can be viewed at: http://usa.visa.com/merchants/risk_management/cisp.html
  Select:
  Visa's Global Registry of Service Providers – PCI DSS Validated Entities List of Validated Payment Applications
- Complete and submit the following documentation to Treasury Management, Payment Card Operations, S-113 Criser Hall, P.O. Box 114050:
  - e-Commerce Application
  - Ethics Certification for each relevant staff member (FA-TM-CCETHICS)

Your application package will be forwarded to the E-Commerce Committee and ultimately to the University Controller's Office for approval.

4.2. e-Commerce Committee Review and Approval

The preferred e-Commerce implementation is through the University web payment gateway (IPAY), together with Higher One's CASHNet product. The department is responsible of developing an interface to the IPAY gateway based on standards specified by the Enterprise Systems liaison of the e-Commerce committee. Any exception to this practice must be approved by the Controller's Office.

The E-Commerce Committee reviews all applications involving credit card sales over the Internet. The committee may include representatives from Finance and Accounting, the Auxiliary Enterprise Review Committee, Enterprise Systems, and the Office of Information Technology.

Applications are reviewed for intended business purpose, consistency with the University's mission, and the selling department's ability to support an e-commerce activity. The proposal will also be judged on its adherence to the Payment Card Industry Data Security Standards (PCI DSS).

Following review and final approval by the University Controller's Office Payment Card Operations will notify the requesting department accordingly, confirm the appropriate chart fields to be credited for sale proceeds, and issue a unique merchant ID or e-commerce profit center identifier for the selling department.

If an exception to an IPAY implementation is approved, the merchant must provide proof that the alternate e-commerce vendor is certified PCI-compliant and ensure that the department and its vendor comply with all relevant provisions of the University of Florida Information Technology Directives, Security Policy and the UF Standards on Credit Cards.

The process to set up an Internet-related account takes approximately 1-2 months.

4.3. Approval of Implementation Changes

Any significant changes to current processes planned by currently active e-commerce merchants must be reviewed and approved by the E-Commerce Committee prior to implementation. Such changes include, but are not limited to changes concerning the

- Departmental website
- Products or services for sale
- Intended customer base
- Anticipated transaction volume
- Outside advertising
- Application software, or
- Departmental contacts responsible for the e-commerce business plan.

Proposed changes should be submitted to Payment Card Operations for review by the Controller's Office.

4.4. Third Party Service Providers

All third party service providers under contract with the University of Florida must be PCI-DSS compliant. Departments who contract with third-party service providers must maintain a list that documents their service providers and:

- Ensures UF contracts/agreements with such providers include language stating that the service provider or third party vendor is PCI compliant and will protect all cardholder data. This requirement also applies if merchants' e-commerce website does not receive cardholder data, but controls how consumers, or their cardholder data are redirected to a PCI DSS-validated third party payment processor.
- Annually confirms the PCI compliance status of all service providers and third-party vendors. A lapse in PCI compliance may result in the termination of the relationship.

4.5. Merchant Fees for Internet-related Account

Please contact your applicable third party provider involved with your e-Commerce implementation to inquire about set up, transaction, and any other recurring fees.

5. Other Considerations

5.1. Publicly Accessible Computers

Publicly accessible computer systems could potentially be used to enter credit card data. If it is part of your daily business process to explicitly encourage or invite customers to use the workstation for payment card processing, you bring such computer system and the entire UF network into PCI scope.

Therefore, if you decide to invite customers to process payment card transactions on any workstation, or assist them in entering payment card data into such a computer system you become liable for addressing well over 300 PCI DSS-related controls.

5.2. IPAY Credit Card Refunds

Credit card refunds that need to be generated to IPAY/CASHNet transactions can be requested with Treasury Management:

Complete form "E-Commerce Credit Card Refund" and submit to Payment Card Operations, Criser Hall S-113, PO Box 114050.

5.3. Annual Self Review

Each merchant processing credit card transactions must complete an annual Self-Assessment Questionnaire (SAQ) to prove compliance with the Payment Card Industry standards (PCI). Payment Card Operations should be notified immediately of any significant changes to credit card business activities or departmental contacts.

5.4. Ongoing Policy Management

The University of Florida may modify these directives and procedures from time to time as required, provided that all modifications are consistent with Payment Card Industry Data Security Standards then in effect.

Payment Card Operations are responsible for initiating and overseeing an annual review of these policy/standards, making appropriate revisions and updates and disseminating the revised directives and procedures to appropriate merchants/UF departments.

6. Loss or Theft, Process for Responding to a Security Breach

Security breaches can result in serious consequences for the university, including the release of confidential information, damage to reputation, added compliance costs, the assessment of substantial fines and possible legal liabilities.

In the event of a breach or suspected breach of security, including the suspicion that credit card information has been exposed, stolen, or misused; the merchant/UF department must immediately do the following:

1. DO NOT turn the compromised terminal off. Instead, quarantine the compromised system from the network by unplugging the communications cord (phone or internet) from the machine. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
2. Preserve logs and electronic evidence
3. Log all actions taken
4. Contact the supervisor/department head
5. Contact Payment Card Operations in Treasury Management at 392-9057
6. Contact the UF Privacy Officer at 1-866-876-4472 (Privacy Hotline)
   The University Privacy Office is located in Tigert Hall, room G-24, Email: privacy@ufl.edu
7. Contact UFIT Security: navigate to my.it.ufl.edu, Technology Services>Information Security>Information Security Investigations>eDiscovery and Forensics, and fill out the form.

The Response Team will immediately coordinate a response and reply to this initial notification/communication to confirm they are aware of the incident. Assist the Response Team as they investigate the incident.

Additional information can be found at:

- http://privacy.ufl.edu
- https://usa.visa.com/support/small-business/data-security.html

6.1. Enforcement - Sanctions

Failure to meet the requirements outlined in these standards may not only result in suspension of the payment card acceptance for affected units, but also in fines and assessments, which may be imposed by the affected payment card company. The responsibility to pay such fines lies ultimately with the impacted unit. In the event of a breach or a PCI violation, the payment card brands may assess penalties to the university's bank, which will be passed on to the university. A one-time penalty of up to $500,000 per branch per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state or federal laws. The University of Florida will carry out its responsibility to report such violations to the appropriate authorities

7. Resources

Forms: http://fa.ufl.edu/forms/

- Request for Credit Card Merchant ID (for usage of swiping machines)
- E-Commerce Application for Credit Card Transactions (FA-TM-ECOMM)
- Ethics Certification (FA-TM-CCETHICS)
- e-Commerce Credit Card Refund (FA-TM-ECCR)

In addition to these standards; any University of Florida employee, contractor or agent who, in the course of doing business on behalf of the university, is involved in the acceptance of credit card and e-Commerce payments for the university is subject to the following policies and guidelines:

- PCI Security Standards Council:
  https://www.pcisecuritystandards.org
- VISA Risk Management:
  http://www.visa.com/visariskproducts/
- VISA "If Compromised":
  https://usa.visa.com/support/small-business/data-security.html
- UF Privacy Office:
  https://privacy.ufl.edu
- UF IT Security Standards:
  http://www.it.ufl.edu/policies/security/

  In particular:

- The Acceptable Use Policy by the Office of Information Technology:
  http://www.it.ufl.edu/policies/aupolicy.html

- UF IT Standards for Data Use Limitations of UF Payment Card Information: http://www.it.ufl.edu/policies/security/documents/use-limitations-pci.pdf

- UF Wireless Network Policy http://www.it.ufl.edu/policies/networking/wireless-network/

- UF Mobile computing and Storage Devices Standard http://www.it.ufl.edu/policies/information-security/mobile-computing-storage-devices/standard/

- UFIT Security Incident Response Procedures http://www.it.ufl.edu/policies/security/incident-response/

Contact Address

Treasury Management – Payment Card Operations
S-113 Criser Hall
PO Box 114050
Gainesville, FL 32611

Phone: (352) 392-9057

Web: http://www.fa.ufl.edu/departments/treasury-management/card-ops/

Email: Treasury-creditcards@ad.ufl.edu