Department Procedure: Payment Card Acceptance

Version:	Modified By Dept.:	Date:	Approved By IA:	Date:
1.0				
2.0				

Department Name: _____ ORG ID: _____

Contact Information:

Department PCI Contact: _____ UNID: _____

Department's Direct Report: _____ UNID: _____

Department's AVP/Dean: _____ UNID: _____

Department Technical Contact: _____ UNID: _____

PURPOSE: The purpose of this policy is to provide guidelines & procedures for accepting payment card transactions (e.g. Visa, MasterCard, American Express, and Discover) by all University of Utah Departments.

PROCEDURES: Payment card processing will be managed to ensure all requirements and policies for accepting and processing card payments are in accordance with the Payment Card Industry Data Security Standard. A designated Department PCI Contact will be required to maintain employee access lists, the department procedures, other applicable PCI DSS documentation, and ensure required training has been completed. All University of Utah employees that process payment cards will follow payment card acceptance procedures as follows:

I. Employee /User Access:

A. Hiring:

1. All employees who will process payment cards will go through the following:
   i. A background check initiated by the Department, through Human Resources, when applicable, for administrative rights to a PCI DSS system.
   ii. Complete/renew annual training: PCI DSS Training & Agreement. Training is accessed through (check one):
      ☐ Learning Management System (LMS) – self-enroll or assigned by department.
      ☐ Financial and Business Services Training Module https://utah.bridgeapp.com/learner/library
   iii. Only designated employees taking payment cards will have access to payment card data, equipment, or other devices in scope for PCI DSS. These individuals will have proper training before being given access to process payment cards.

B. Termination:

1. Termination will be conducted by the hiring department and Human Resources. Once termination has been decided, the department PCI Contact will record the termination date of the employee and request removal from all PCI access, including, but not limited to the following:
   i. Departmental Deposit Access
   ii. 3rd Party Software or Point of Sale Device
   iii. UMarket or other e-Commerce Web Portal
   iv. WIAN Active Directory

C. A complete, dynamic list of employees that process payment cards will be kept by the Department PCI Contact (see Attachment A), including hire/termination dates, training, and the employee roles and

responsibilities regarding payment card processing. As changes are made, a copy is given to Income Accounting and Student Loans. Employee roles and responsibilities within the department are as follows:
(Roles may include: cashier, manager, supervisor, accountant, etc. Lines may be added to the table as needed.)

Roles	PCI Responsibilities

II. Security:

A. All new merchant accounts and changes to processing methods will be approved by Income Accounting and Student Loan Services.

B. Where applicable, servers, and ancillary devices are located in the University of Utah Data Center.

C. Computer Access ☐ (check if applicable):

1. Each person with access to computers used for payment card processing will have their own unique ID and password. Sharing passwords is expressly forbidden.
2. Passwords will be maintained in accordance with the University's password guidelines by using a password, phrase, upper and lower case letter, numbers, and special characters. Vendor supplied passwords will never be used.
3. Passwords should not be stored in either paper or electronic form.
4. Passwords should be changed at least every 90 days.
5. Users who use computers in scope for PCI must have access to the WIAN PCI Active Directory.
    i. Supervisors will use the WIAN Security Authorization Request Form
    ii. Employees with administrative access to the department PCI devices must have a background check.
        a. All background checks are initiated with Human Resources (HR) by the department.
        b. Background checks are verified with HR by Income Accounting and Student Loan Services.
    iii. Income Accounting and Student Loan Services approves or denies access to the WIAN PCI Active Directory.
    iv. WIAN Access will be deactivated after 90 days of inactivity.

D. Other PCI Devices (check all that apply):

☐ Stand Alone Terminal (dial-up or IP):

1. Terminals are kept in an area that is not easily accessible to the public.
2. Terminals are regularly inspected for skimming devices and/or other physical tampering.
3. IP terminals are configured with a static IP address behind the University PCI firewall.
4. The serial number of each terminal will be maintained by the PCI Contact, and reported to Income Accounting and Student Loans annually. See VIII.
5. A monthly inspection of the terminal will be completed and logged to identify any physical tampering of the device including the swiping mechanism and/or EMV slot. See Attachment B.
6. Replacement terminals will be requested through Income Accounting and Student Loans.

☐ End to End or Point to Point Encrypted Devices:

1. All encrypted devices will be approved and tested by the University.
2. The serial numbers of the encrypted devices must be inventoried annually by the department or the accounting area the department reports to (i.e. Income Accounting and Student Loans, Pharmacy Administration, or UUHC Accounting.) See VIII.
3. A monthly inspection of the swipe and/or EMV slot will be completed and logged to identify any physical tampering of the device. See Attachment B.
4. New or replacement encrypted devices will be requested through the applicable accounting area.

☐ Other Point of Sale Devices:

1. Register systems integrated with approved PCI DSS Compliant 3rd Party Vendor Payment Applications or Service Providers.
    i. Each person with access to computers used for payment card processing will have their own unique ID and password. Sharing passwords is expressly forbidden.

ii. Passwords will be maintained in accordance with the University's password guidelines by using a password, phrase, upper and lower case letter, numbers, and special characters. Vendor supplied passwords will never be used.
iii. Passwords will not be stored in either paper or electronic form.

2. Passwords will be changed at least every 90 days.
3. A monthly inspection of the swiping mechanism and/or EMV slot will be completed and logged to identify any physical tampering of the device. See Attachment B.

E. Incident Response:
1. Suspected or verified PCI violations will be responded to using the University of Utah's Department Incident Response Plan Procedure – Standard 12.9.
2. The department will annually review the University Department Incident Response Plan Procedure.

III. Payment Card Data Handling (check all that apply):

A. Department receives payments in the following manner:

☐In Person – swiped/inserted/tapped

☐Mail

☐E-Commerce Application – UMarket or approved E-Commerce 3rd Party Vendor.

☐Fax (fax is maintained in a secure area, with limited access and is not connected to the internet). Receiving payment card data via fax is discouraged.

☐Phone

i. The phone system is called ☐.
ii. The phone system is Voice Over IP ☐ Yes ☐ No
iii. The phone calls are recorded ☐ Yes ☐ No

B. Payment Card Data only accepted via In Person, Mail or by Phone.
1. Payment Card Data is never accepted via Email. If payment card data is erroneously received, the email will be deleted immediately from the email inbox, and the deleted folder.
2. Payment Card Data is never accepted via Fax, especially if connected to the internet.
3. Payment Card Data is never accepted via Instant Messaging, including MyChart.

C. All payment cards are processed immediately, or within one business day.

D. The 3 digit security code on the back of the card and the expiration date is never stored on paper or electronically.

E. The last four digits of the payment card number may be retained.

F. Truncated payment card receipts and settlement reports should be retained for one year in case of cardholder disputes.

G. All paper forms used to collect payment card data are formatted so the data can be easily redacted or removed for cross-cut shredding.

H. Redacting payment card data is completed in the following manner:
1. The payment card number is removed from the paper form, if applicable, and is immediately cross-cut shredded, ***or***
2. The payment card data is blacked out as thoroughly as possible. The paper form is then copied and the copy is stored. The original form is immediately cross-cut shredded.
3. Forms that are appropriately redacted or truncated may be retained for the length of time deemed necessary by the department.

I. All payment cards are settled daily for deposit.

J. E-Commerce transactions are cardholder initiated transactions. Employees will not process transactions through their E-Commerce application on behalf of the cardholder.

K. Payment Card Data Storage:
1. Payment Card Data is only stored temporarily, not to exceed 1 business day, in order for authorization and settlement to occur.
2. Payment Card Data is only stored in a secured, locked area, with limited access, prior to authorization. Payment Card data is never stored in paper form following authorization.
3. Un-redacted payment card data is never sent to University Archives or other records storage facilities.
4. Payment Card Data stored electronically is done so in accordance with the PCI DSS.

5. Payment Card Data cannot be stored on the following devices:
    i. Computers, personal or University owned
    ii. Application or program that runs on a desktop workstation
    iii. Jump or Flash Drives
    iv. Non-PCI approved Devices
    v. A rolodex or other type of manual system

IV. Payment Card Processing (check all that apply):

A. ☐Card Not Present Transactions
    1. When applicable, keep your computer, or card processing device out of the line of sight of others.
    2. Payment card information should only be written down if card data cannot be entered directly in the computer or other card processing device, or card information was received on a form or through the mail.
        i. After the transaction is authorized, all but the last four digits of the payment card number should be redacted appropriately (see II.H), or removed from the form and cross-cut shredded.
        ii. Written payment card data must be authorized immediately, or within one business day of receipt. Any payment card numbers that are kept overnight will be locked in a secure area with limited, need to know access.
    3. The cardholder's billing zip code should be entered for address verification.
    4. If the card is declined, the card may be run one more time to verify the decline was not caused by data entry.
    5. Employees will not ask for payment card information to be emailed or faxed.
        i. If faxed payment card information is received, redact or cross-cut shred after the transaction has been authorized.
        ii. If emailed payment card information is received, promptly delete the email from your in-box and deleted folder after the payment card number has been authorized.

B. ☐ Card Present Transactions:
    1. When applicable, keep your computer, or other card processing device out of the line of sight of others.
    2. Swiping/inserting/tapping the card is the most secure method of accepting payment cards. If the card will not except electronically, key enter the payment card information manually into the P2PE card reader or other payment processing device.
    3. If the card is declined, the transaction must not be run again. Ask for another form of payment.
    4. If an EMV (aka Chip and PIN) card is presented and the PCI device is enabled for this processing method, the card will be processed as an EMV card.

C. ☐V Pay:
    1. V Pay is a one-time use payment card number received via mail, fax, or secure website.
    2. V Pay card data will be processed within 1 business day of receipt.
    3. V Pay card data will be appropriately redacted (see II.H) or removed and cross-cut shredded. The last 4 digits of the card number may be kept.

D. Refunds:
    1. Refunds must be issued using the same mode of processing that was used for the original transaction.
    2. Refunds must be issued to the same payment card number that was used for the original transaction.
    3. If the card holder can provide documentation that the original payment card account number has been closed, the department may issue a refund via a Payment Request through Accounts Payable.
    4. The refund amount may only be up to the amount of the original transaction.
    5. Refunds must be approved by a supervisor, for dual control, by the supervisor signing the refund receipt attached to the original transaction receipt.

E. Retrieval Requests:
    1. Retrieval Requests represent payments that are disputed by a cardholder in which receipts and all applicable transaction documentation are requested.
    2. Retrieval Requests may be received vial mail, fax, or by Income Accounting and Student Loans.

3. If the full payment card number is received, it must be properly redacted, leaving only the last four digits.
4. The department will gather all receipts and applicable transaction documentation to return to Merchant Services via fax. No un-redacted payment card numbers will be faxed.
5. The department will respond to the Retrieval Request before the due date. Otherwise, the retrieval request will be charged back to the department, by Merchant Services, for non-receipt of requested information.
6. If a refund for the disputed transaction is deemed appropriate, the department will follow the refund procedure.

F. Chargebacks:
1. Chargebacks represent payments that are disputed by a cardholder, and the transaction amount has been debited from the department account.
2. If the full payment card number is received, it must be properly redacted, leaving only the last four digits.
3. The department may dispute the chargeback by the due date on the chargeback documentation if the chargeback is deemed inaccurate.
4. The department will gather all receipts and applicable transaction documentation to return to Merchant Services via fax or online. No un-redacted payment card numbers will be faxed.
5. A refund must not be processed as the bank account has already been charged by Merchant Services.
6. The department will book the negative amount of the chargeback through their applicable method: appropriate accounting department or departmental deposit to Income Accounting and Student Loans. A copy of the chargeback documentation will be provided as back-up.
7. Reversed Chargebacks will be booked, by the department, as a deposit through their applicable method: appropriate accounting department or departmental deposit to Income Accounting and Student Loans. A copy of the chargeback reversal documentation will be provided as back-up.

V. Change Management ☐ (check if applicable):

Modes of processing that require Change Management are: 3rd Party Software hosted on Campus, Virtual Terminals, Kiosks, Re-Directed Software or applications, and IP Terminals.

A. All changes and updates to the operating system, hardware, IP, or software of a PCI system are categorized as one of the following. The UIT procedures will be followed for each change.
1. *Standard Change:* Well documented, low risk, and proven. Standard changes are done on a regular basis and been implemented successfully multiple time before. The first instance of a standard change needs to be submitted and reviewed by the CAB before implementation. Afterwards, standard changes are considered pre-approved and can be implemented during the next available change window without CAB approval or using required lead times. Coordination activities can be done at the discretion of the Systems Analysts.
2. *Minor Change:* A minor change has a low impact either in terms of the number of users affected or the criticality of the service and has a low risk of failure. Minor changes are reviewed by the Change Management team and approved by the Change Manager. Minor changes need to have the required lead time. Coordination activities can be done at the discretion of the Systems Analysts.
3. *Major Change:* A major change has significant impact on users or services, a high risk of failure, or is complex and requires multiple teams to implement. This may also include new, high-profile applications that are being used in production for the first time or changes to applications where a high degree of coordination between multiple organizations needs to occur.
4. *Emergency Change:* This is a change that needs to be implemented IMMEDIATELY to fix an incident due to severe loss in service capability.
5. *Significant Change:* May include standard, minor, major or emergency changes. **From PCI Guidance:** The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Refer to Significant Change Requirements.

B. All changes are documented in the following system (check one):
1. ☐UIT Change Management System.
2. ☐Department Change Management System *approved by a Qualified Security Assessor*.

C. All Changes require the following steps, as applicable to the change category:
   1. Complete a Request for Change (RFC) to UIT.
   2. Contact Security Assurance Group.
   3. Request any applicable firewall changes as part of RFC.
   4. Update data flow diagram and network diagram.
   5. Update Asset Inventory in Department Box Folder.
   6. Complete a Penetration Test as applicable.

VI. Vulnerability Scans ☐ (check if applicable):

A. Internal PCI Vulnerability Scans are run on a weekly basis by the Information Security Office.

B. External Scans are conducted for all public facing systems. ☐(check if applicable):
   1. External Scans will be completed at the beginning of each month.
   2. The external scans will be repeated weekly until the scan is passing and can be attested by Qualys.

C. All vulnerabilities will be addressed within a maximum of 30 days of the finding.
   1. False Positive vulnerabilities will be documented as such. Documentation will be uploaded to the department PCI Box Folder.
   2. True vulnerabilities will be remediated as soon as possible, and no later than 30 days of the finding.

D. Any changes to IP addresses, additions, and deletions will be documented through an RFC, and the Information Security Office will be notified to make the changes for the vulnerability scans.

VII. Penetration Testing ☐ (check if applicable):

Modes of processing that require Penetration Testing are: 3rd Party Software hosted on Campus and Re-Directed Software or applications. Others modes will be tested as deemed necessary by a Qualified Security Assessor.

A. A Penetration Test will be completed by qualified personnel, internal or externally contracted, on the applicable PCI systems at least once a year.

B. Any significant changes to the PCI System, as defined in V.A.5, must be followed by a penetration test, to be initiated within 30 days of the significant change.

C. Any findings that may pose a risk of breach to the system, or do not meet standard best practices, will be remediated within 30 days of the finding. Testing of the remediation will follow.

VIII. Asset Inventory

A. A complete inventory of PCI devices and components must be kept current by the PCI Contact.

B. Any changes made to the PCI devices inventory will be updated immediately and a copy sent to Income Accounting and Student Loan Services.

C. A monthly inspection of all swipe and EMV capable devices will be completed and logged. See Attachment B.

D. The asset inventory includes, but is not limited to the following:
   1. Serial Number of each PCI device
   2. Make and Model of each PCI device
   3. Location of each PCI device
   4. Purpose of each PCI device
   5. IP addresses
   6. VLANs
   7. MAC address
   8. Firewalls

E. ☐(check if applicable) Asset Inventory for Stand Alone Terminals, IP Terminals, P2PE and E2EE devices:
(Lines may be added to the table as needed.)

Serial Number (i.e. NT0000007233)	Tamper Tape #	Make/ Model (i.e. FD100Ti)	Location (i.e. front desk)	IP Address (IP terminals only)

F. ☐(check if applicable) Asset Inventory will be updated in the department Box Folder.

IX. Addendums ☐ (check if applicable):

A. Addendums have been added for specific PCI procedures for the department not listed in this procedure.

X. Attachments:

A. Employee List

B. Monthly PCI Device Inspection Log

C. Department Form(s) for payment card collection ☒ (check if applicable)