Training Agenda

• Introduction
• PCI DSS Compliance
• Department Responsibilities
• How to use your payment card machine
• What to do if you need more services...
• Best practices to use when accepting payment cards

Contact Information

• Kim McClellan
  Administrative Program Coordinator
  Income Accounting & Student Loan Services
  kim.mcclellan@utah.edu
  585-5686
• Lisa Zaelit
  Accounting Manager
  Income Accounting & Student Loan Services
  lisa.zaelit@admin.utah.edu
  581-3968
What is PCI DSS?

The PCI DSS version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.
The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Payment Card Industry Data Security Standard (PCI DSS)

Build and Maintain a Secure Network
- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
- Requirement 12: Maintain a policy that addresses information security
Benefits & Reasons to Comply

• Protection of all payment card information.
• It is the responsibility of the University, as a business, to maintain security and best practices.
• The University is very complex because of all the different needs and processes of each department.
• Significant monetary consequences for non-compliance.
• Significant public relation consequences for non-compliance.

Department Requirements

• Annual Questionnaire
• Annual Terms of Use Agreement
• Annual Training
• Departmental Best Practices Procedures
• Department Contact Information

U MERCHANT PACKETS
Thank you.

Please click on the links below to view and complete the necessary documents.

Contents:
- Administration Letter & PCI Requirements
- UNIVERSITY PAYMENT CARD ACCEPTANCE/ E-COMMERCE POLICY
- Items to Complete and/or Return to Income Accounting & Student Loan Services:

Instructions:

Summary

Summary of PCI DSS Requirements

You are being notified of PCI DSS requirements as the University of Utah expands its acceptance of credit cards. A vast number of data breaches, many involving credit card numbers, have occurred in the past. As of May 2006, credit card issuers and their associations, the card brands (Visa, MasterCard, American Express, Discover, JCB, and Diners Club International), have established, and required all merchants to comply with the Payment Card Industry Data Security Standard (PCI DSS). This standard is designed to protect the confidentiality, integrity, and availability of the cardholder's data, and to establish a secure environment in which to transact credit card payments.

The PCI DSS presents a comprehensive set of requirements that are intended to achieve the following objectives: Preventing disclosure of cardholder data, Protecting cardholder data, Safeguarding cardholder data, and Maintaining a secure network. These requirements affect all aspects of the merchant's business, including the business processes involved in storing, processing, and transmitting cardholder data. All businesses are expected to implement and maintain a security program that includes the development and implementation of policies and procedures. The consequences of non-compliance include fines, legal action, and damage to customer confidence.

WHAT IS PCI DSS?

The PCI DSS standard is a set of requirements established by Visa, MasterCard, American Express, Discover, JCB, and Diners Club International. It is designed to protect the confidentiality, integrity, and availability of the cardholder's data, and to establish a secure environment in which to transact credit card payments. The standard includes requirements for secure network administration, physical and environmental security, access control, password management, personnel security, software and configuration management, and incident handling.

Existing Merchant Information Packet (B)

Department Name: [Insert Department Name]
Completed by: [Insert Name]

- Copy of Department Reconciliation Policy
- Terms of Use Agreement Completed via EDUCAT
- Change Form
- UNIVERSITY PAYMENT CARD ACCEPTANCE/ E-COMMERCE POLICY

Items to Complete and/or Return to Income Accounting & Student Loan Services:

- Administrator's Letter
- Department's Name: [Insert Department Name]
- Completed by: [Insert Name]
- Date: [Insert Date]
- University of Utah
- 201 South 1460 East
- Rm 155
- Salt Lake City, UT 84112
- 801-585-1234

UNIVERSITY PAYMENT CARD ACCEPTANCE/ E-COMMERCE POLICY

The Payment Card & E-Commerce Acceptance Policy is being established, and procedures are being updated to assist departments in properly handling payment card transactions. You will be notified as soon as this is available for you to review.

Current Guidelines:
http://bs.admin.utah.edu/download/guidelines/CreditCardGuidelines.pdf
A contact person, a cognizant authority, and/or a Dean/VP/Director must be identified and take part in the management of each department’s payment card processing. They will ultimately be held accountable for ensuring PCI compliance and maintaining proper reconciliation processes within their own department.

Upon the approval of Income Accounting and Student Loan Services, departments wishing to engage in e-commerce must use an authorized University payment application or offer evidence that an approved, alternate vendor meets University requirements and PCI DSS standards.
All suspected or actual security breaches of payment card or other e-commerce information must be reported immediately to Income Accounting and Student Loan Services. Please see, University of Utah Policy 1-18, University Information Technology Resource Security Policy for additional reporting requirements.

**SELF-ASSESSMENT QUESTIONNAIRE**

- Link to Questionnaire
- Use your UNID and password to log in
- Answer all questions “Yes” or “No”
- Obtain help from your IT Advisor, if needed
- Call Income Accounting & Student Loan Services for help
- Must be completed by October 25, 2008

**TERMS OF USE AGREEMENT**

Payment Card Industry Data Security Standard (PCI DSS) Terms of Use Agreement

1. I have read and understand the PCI DSS Requirements outlined in this agreement.
2. I agree to keep all contact information updated.
3. If applicable, I agree to cooperate with any security scanning of the servers or computers in my department involved in payment card processing.
4. I agree to comply with the preceding policy, and any new requirements set forth by the university and/or the PCI DSS Requirements.
5. I recognize that failure to comply with the PCI DSS Requirements may result in termination of the department’s payment card merchant account.

"Affirmation that you have reviewed these policies and procedures satisfy PCI DSS Requirement 12.6.2: "Require employees to acknowledge in writing that they have read and understood the company’s security policy and procedures.”"

\[YES\]  \[NO\]
RECONCILIATION
The “Why” and “How”

WHY?

• Since each daily settlement is a deposit, chart fields should be credited within three days to ensure that all deposits are booked promptly.

• This assures that all monies are deposited accurately to the bank account for monthly bank reconciliation purposes.

http://fbs.admin.utah.edu/index.php/ecommerce/
• All payment card machines must be settled daily.
• The summary/settlement tape is proof of deposit and is the back-up that must be provided with the departmental deposit form.
• Each card type total is a deposit. Visa/Mastercard, Discover, and American Express are the three credit card deposit types you will have.
• Departmental deposits should be prepared and taken to the Cashier’s office daily.

When your needs change.....

We have some ideas!
**U**Pay

- Created by the University
- Preferred Payment Application
- Uses a secure, certified server – PCI Compliant
- Deposits post directly to your chart fields
- Simple reconciliation

---

**U**Market

- Check-Out Page
- Shopping Cart
Advantages to UMarket

- Website is hosted on a secure, certified server
- Both the shopping cart and the checkout page can be customized
- Simple to modify
- Available template, a whole website does NOT have to be built.
- You can have both UMarket options with one account.

USING A THIRD PARTY VENDOR

- Third Party = software or internet connection to a system that collects card information and other sensitive data.
- Third Party Vendors MUST be PCI Compliant
- Approved List on Website
- Exception Requests

HOW TO ACCEPT PAYMENT CARDS
CARD PRESENT

CARD NOT PRESENT

INFORMATION STORAGE

- Need to know access
- Locked
- NO encrypted emails
- Department Policy
- No written card #’s
- Terminals out of reach
- Truncation
PAYMENT CARD ACCEPTANCE & 
eCOMMERCE WEBSITE
http://fbs.admin.utah.edu/index.php/ecommerce/