University of Notre Dame
Credit Card Support Program
Merchant Manual
Version 1.09

CREDIT CARD SUPPORT PROGRAM
200A Information Technology Center
Notre Dame, Indiana 46556
Email: ccsp@nd.edu
Tel: (574) 631-3503
Fax:(574) 631-9283

PCI Security Standards Council
PARTICIPATING ORGANIZATION
# TABLE OF CONTENTS

**PAYMENT CARD INDUSTRY/CREDIT CARD SUPPORT PROGRAM OVERVIEW** .......................... 3

**UNIVERSITY OF NOTRE DAME PAYMENT CARD POLICIES AND STANDARDS** ................. 10
  UNIVERSITY OF NOTRE DAME PAYMENT CARD POLICY ........................................ 12
  BUSINESS STANDARDS FOR PAYMENT CARD PROCESSING .................................. 17
  TECHNICAL STANDARDS FOR PAYMENT CARD PROCESSING ............................... 21
  THIRD PARTY-VENDOR GUIDELINES ................................................................. 33

**UNIVERSITY OF NOTRE DAME PAYMENT CARD PROCESSING PROCEDURES** ............... 35
  MERCHANT ACCOUNT ACQUISITION PROCEDURES .............................................. 37
  PAYMENT CARD DATA HANDLING PROCEDURES .............................................. 39
  PAYMENT CARD RECONCILIATION PROCEDURES ............................................. 42
  PAYMENT ENVIRONMENT CHANGE APPROVAL PROCEDURE ................................ 46
  POSITION MODIFICATION PROCEDURE ............................................................. 48
  CCSP DATABASE UPDATE PROCEDURE ............................................................. 51

**PAYMENT ACCEPTANCE METHODS** ........................................................................... 53
  E-COMMERCE: THE NOTRE DAME MARKETPLACE ........................................... 55
  CARD PRESENT & MAIL ORDER/TELEPHONE ORDER (MOTO) TRANSACTIONS ........ 56
  VIRTUAL TERMINALS ......................................................................................... 57
  OTHER PAYMENT ACCEPTANCE OPTIONS ......................................................... 58
  MOBILE PAYMENT APP ...................................................................................... 59

**CCSP FORMS** ...................................................................................................... 61
  MERCHANT CONTACT INFORMATION FORM .................................................... 63
  REGISTRY OF CARD PROCESSING DEVICES ..................................................... 64
  BUSINESS CONTINUITY PLAN TEMPLATE COVER PAGE .................................. 65
  PAYMENT ACCEPTANCE ACTIVITY CLARIFICATION FORM ............................... 66
  BUSINESS PROCESS ASSESSMENT ..................................................................... 67
  POLICY ATTESTATION FORM ............................................................................. 68
  SERVICE PROVIDER ASSESSMENT .................................................................... 69
  PCI SECURITY BACKGROUND CHECK AUTHORIZATION FORM .......................... 70
  QUARTERLY NETWORK INSPECTION TEMPLATE ............................................. 71
  SAMPLE EMAIL RESPONSE ................................................................................ 72

**FREQUENTLY ASKED QUESTIONS** ................................................................. 74
**GLOSSARY** .......................................................................................................... 79
**TRAINING** ........................................................................................................... 86
**EXTERNAL RESOURCES** ....................................................................................... 90
Section 1: PCI/CCSP Overview
What is PCI DSS?

The Payment Card Industry Data Security Standard, or PCI DSS, is a set of comprehensive requirements for enhancing payment account data security. It 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 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. It contains over 200 specific security requirements, broken down into 12 different categories.

Who does PCI DSS apply to?

All merchants and service providers who process, store, or transmit cardholder data are required to adhere to PCI DSS. This is enforced through contractual requirements passed down from the card brands to all merchants through their merchant (acquiring) banks.

Why is it important to comply with the PCI DSS?

There are contractual, ethical, and financial reasons for adhering to the PCI DSS.

- Contractual: Notre Dame’s acquiring bank mandates that all merchants not only comply with the PCI DSS at all times, but also validate that compliance. In order to validate compliance with the standard, a “Self Assessment Questionnaire” (SAQ) must be completed annually. If a merchant does not adhere to all PCI requirements, and/or does not validate that those requirements are being met in a timely fashion, then the University is in breach of its contract and the merchant bank may choose to close the offending merchant account immediately, restricting the merchant from collecting any credit card information as a form of payment.

- Ethical: When a merchant accepts a credit card, the customer trusts that their sensitive personal data is being protected. Only by complying with PCI DSS can merchants ensure that they are adequately protecting that data.

- Financial. A 2011 Ponemon Institute study estimates that data compromises cost merchants on average $204 per affected customer. \(^2\) Since a payment application (especially a non-compliant one) may have years worth of sensitive customer data, the

---

number of affected customers, and the cost of a breach, can be very large. It is impossible to identify the exact cost of a breach before it happens though. Instead, we can identify the types of costs that you as merchant and the university as a whole would incur.

1. Incident Response and Cleanup: This includes lost employee productivity as university resources are reallocated to analyze what happened, contain the problem, repair information systems, and collect forensic evidence.

2. Notification Costs: All customers who may have been affected by the data compromise must be notified, and the university may need to offer each of these customers credit monitoring services for a minimum of one year.

3. Regulatory fines: The card brands levy fines on the acquiring banks for mismanaging customer data, which the acquiring bank then will pass onto the responsible merchant. These fines could range from several thousand to several million dollars, depending on the size and the severity of the breach.

4. Opportunity Costs: Forrester Research estimates that 10-20% of potential customers will be lost due to a security breach in a given year.

5. Audit Costs: After a breach, merchants may be required to be audited by a qualified third party assessor for a minimum of one year. The cost of this outside assessment is significantly higher than the cost of assessing ourselves internally.

6. Other liabilities: Credit card replacement and civil penalties for those affected can potentially add to the already significant costs of a breach.³

It’s possible to view the importance of PCI Compliance from several different perspectives, but only by looking at the issues from contractual, ethical, and financial perspectives can you begin to see the big picture of why it is so important for all of us as an institution to adhere to the PCI DSS.

What is the role of the Credit Card Support Program (CCSP)?

The PCI DSS is cross-functional by its very nature. In order to fully protect credit card data, both technical and business related requirements must be followed. For example, from the business side, proper mail and paper handling procedures must be followed, and employees must receive background checks prior to employment; from the technical side, proper network encryption and firewall settings must be followed. These cross-functional requirements make it understandably difficult for a single merchant to ensure and verify all aspects of their compliance.

The Credit Card Support Program oversees several activities that help merchants maintain their PCI DSS Compliance. The CCSP centrally manages the following:

**Account Management:** Computer accounts for individuals that can access *cardholder data* must be managed to a strict standard, and require multi-factor authentication for access. The CCSP manages these accounts and assists users with their accounts, passwords, or *tokens*.

**SAQ Submission:** The CCSP helps to coordinate all of the activities required for merchants to validate PCI DSS compliance and submit SAQs. Rather than requiring that each individual merchant work with HR, Information Security, and other departments to answer the SAQs in full, the CCSP Office has divided the SAQs into department specific assessments. (Some of these assessments can be found in Section 5 of this document.) This way, the merchant only needs to answer applicable questions, while the other assessments are answered by the appropriate subject matter experts. The CCSP office aggregates all of the assessment answers into the SAQ, requests approval from the appropriate officer responsible for the merchant activity, and then submits the SAQ to the bank. This process occurs once per year for every merchant at the University. (Some departments manage more than one merchant account.) The timing of this process will vary depending on your merchant account.

**New Merchant Approval:** Before the University’s merchant bank will permit any funds to flow though a new merchant account, they must verify that certain security measures consistent with PCI DSS are in place. The CCSP facilitates this new account setup and ensures that the merchant can and will comply with PCI DSS. As part of this process, all proposed merchant activity is reviewed by the Information Governance Committee and approved by the Vice President Finance.

**Payment Environment Change Approval:** Because a merchant’s payment environment is typically not static and can require changes to scope, technology, location, etc, it is possible for a merchant that was once meeting the PCI DSS to become non-compliant. To prevent this from happening, the Information Governance Committee must review all proposed changes to the campus payment environment.

**PCI DSS Awareness:** The CCSP oversees a multifaceted security awareness program, which includes, among other things, online training, an informational website, merchant meetings, and this manual. In addition to the clear benefit of educating campus merchants about credit card security, having such an awareness program is a requirement of the PCI DSS.
Who is the Information Governance Committee?

The purpose of the Information Governance Committee is to ensure that all requirements of the PCI DSS are met, and to guarantee that all necessary stakeholders review any card processing activity or change in card processing activity before implementation. The Committee ensures that merchant activities are aligned with University goals and policies.

David Bailey  
Strategic Planning Program Director  
Office of Strategic Planning  

Mike Chapple  
Senior Director Enterprise Support Services  
Office of Chief Information Officer  

Timothy Flanagan  
Associate General Counsel  
Office of General Counsel  

Tamara Freeman  
Director Talent Management & HR Strategy  
Office of the Controller  

Todd Hill  
Senior Director Academic & Administrative Services  
Office of Chief Information Officer  

Chuck Hurley  
University Registrar  
Office of the Registrar  

Micki Kidder  
AVP Development Advancement Services & Finance  
Office of Development Services  

Ron Kraemer  
VP & Chief Information and Digital Officer  
Office of Information Technology  

Roger Mahoney  
Director Audit & Advisory Services  
Office of Audit & Advisory Services  

Drew Paluf  
AVP Controller  
Office of the Controller  

Matthew Blazejewski  
EVP Senior Advisor  
Office of Executive Vice President  

Liz Rulli  
AVP Research  
Office of Research  

Scott Kirner (standing guest)  
Director Application Development  
Office of Information Technology
Section 2: University of Notre Dame Payment Card Policies and Standards
University of Notre Dame Payment Card Policy

Merchant Account Acquisition and Usage

All card processing activities of the University of Notre Dame will be conducted through merchant accounts obtained through the Merchant Account Acquisition Procedure.

Notre Dame merchant accounts will be issued only to particular Notre Dame entities for a specific use. Accounts operated by parties other than the approved entity or for a purpose other than that approved may be rescinded without notice.

Protection of Cardholder Information

All card processing activities and payment technologies of the University of Notre Dame must comply with the Payment Card Industry Data Security Standard (PCI DSS) as described in the Notre Dame payment card standards and procedures. No activity or technology may obstruct compliance with the PCI DSS.

Through regular meetings with the Operational Oversight Committee and related working groups, the Credit Card Support Program (CCSP) will conduct an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.

The University will screen potential employees to minimize the risk of attacks from internal sources.

The University will contractually require all third parties with access to cardholder data to adhere to PCI DSS requirements. These contracts will clearly define information security responsibilities for contractors.

Alteration of Card Processing Environment

Any alteration of the card processing environment must receive explicit written approval through the Payment Environment Change Approval Process. Changes include but are not limited to:

- the use of existing merchant accounts for new purposes,
- the alteration of business processes that involve card processing activities,
- the addition or alteration of payment systems,
- the addition or alteration of relationships with third-party payment card service providers,
- the addition or alteration of payment card processing technologies or channels.
Cellular Modem and Wired-Analog Modem Uplink Devices and Usage

For changes involving the use of cellular wireless technology or the installation of analog wired modems on systems that store, process or transmit cardholder data, the following details must be provided to complete the Payment Environment Change Approval Process:

- A description of authentication technology in place,
- A list of all devices and personnel with access,
- For wired modems, a proposed connectivity time-out period (All modems must automatically disconnect sessions after a specified period of inactivity.)

Approval of the change will include:

- Specific acceptable use(s) chosen for the technology
- Specific approved network location(s) for the technology
- Specific approval of the product(s) used

In general, the University disallows and discourages the use of cellular wireless uplink technology for card processing activities. If approved, all devices will be labeled with the owner, contact information, and purpose of the device, prior to deployment of the technology.

802.11 Wireless LANs will not be connected to, or part of, the cardholder data environment.

When accessing cardholder data remotely via wireless or wired modem, it is prohibited to store cardholder data on local hard drives, floppy disks or other external media. It is also prohibited to use cut-and-paste and print functions during remote access. Activation of modems for vendors will occur only when needed, with immediate deactivation after use.

Applicability

This policy applies to all University of Notre Dame employees and students.

Responsibilities

The CCSP will:

1. Establish, document and distribute security policies and procedures.
2. Make all employees aware of the importance of cardholder information security through a formal security awareness program.
3. Assist merchants with the completion and submission of all PCI-DSS Self Assessment Questionnaires.
4. Administer the Payment Environment Change Approval Process wherein changes to the payment environment are approved by Information Governance Committee and/or by the Vice Presidents for Finance and Business Operations.
5. Administer the Merchant Account Acquisition Procedure wherein new accounts are approved by the Information Governance Committee.
6. Maintain a current list of service providers, and procedures to manage those service providers.

**OIT Information Security will:**

1. Establish, test, document, revise as needed, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
2. Monitor and analyze security alerts and information and distribute to appropriate personnel.
3. Information Security will conduct an annual risk assessment of the CCSP. The assessment will identify threats and vulnerabilities, and will include input from managers, administrators, and users of the environment. The results of the assessment will be documented and available for review.

**Administrators of card processing systems and applications will:**

1. Administer user accounts, including additions, deletions and modifications.
2. Monitor and control all access to data.

**Merchants will:**

1. Ensure that all of their employees and business processes comply with this policy and related procedures.
2. Identify positions that require access to cardholder data, specifying positions with access to multiple instances of cardholder data.
3. Notify Human Resources through their department’s HR Business Partner and the CCSP of all staff changes in positions with Privileged Access to Cardholder Data.
4. Make their employees aware of the importance of cardholder information security.

**Human Resources will:**

1. Screen potential employees in identified positions to minimize the risk of attacks from internal sources.

**Office of Information Technologies will:**

1. CCSP technical duties and privileges are assigned by job classification and function. The following CCSP roles have been assigned to these departments or groups:
   - Server OS engineering and administration: EIS System Services
   - VMWare engineering and administration: EIS System Services
   - Network engineering (not firewall): EIS Network Services
   - Active Directory engineering: EIS Directory Support
   - Firewall services: ESS Information Security
   - Monitoring and testing: ESS Information Security
   - Desktop support: CSS Desktop Support and Desktop Engineering
• Application administration: merchants

**Review**
CCSP will review this policy and related procedures annually. This policy and related procedures will be updated when the card processing environment changes.

**Exceptions**
Exceptions to this policy or related procedures must be approved through the Information Governance Committee.
Business Standard for Payment Card Processing

Account Acquisition

Notre Dame merchant accounts will be issued only to particular Notre Dame entities for a specific use and must be obtained through the Merchant Account Acquisition Procedure.

Roles and Responsibilities

Each merchant must identify individual(s) to fill the following roles for each merchant account. (An individual may fulfill multiple roles.)

**Director**
The Director of the area is responsible for ensuring that employees are familiar with and adhere to all payment card policies, standards, and procedures. The Director may need to approve change requests made through the Payment Environment Change Approval Process.

**Account Owner**
The Account Owner is the primary contact for merchant account communications issued by the merchant bank and the CCSP. To facilitate the annual completion of the industry required Self Assessment Questionnaire (SAQ), the Account Owner is responsible for maintaining and providing certain information to the CCSP upon request. Specifically, the Account Owner must:

- complete the Business Process Assessment (a brief, yes-no-N/A questionnaire)
- maintain the Registry of Card Processing Personnel
- report position changes (as described below)
- assist in identifying other departmental resources, as necessary to complete the SAQ
- act as the merchant’s Business Continuity Coordinator

**Business Manager**
The Business Manager is responsible for reconciliation of all operating accounts where payment card revenue is deposited. Where revenue is credited to an unearned revenue account, the Business Manager is responsible for transferring funds to the appropriate operating ledger account(s). Detailed reconciliations are to be maintained by the business manager. The Merchant Card Coordinator should be contacted for assistance or questions regarding reconciliation. (See Payment Card Reconciliation Procedures.)

**IT Contact**
The IT Contact will maintain the Registry of Card Processing Devices for all merchant equipment attached to the card processing environment. The registry must be available to
the CCSP upon request. The IT Contact will assist in completing the technical sections of the annual Self Assessment Questionnaire, if necessary.

Changes to contact information for these roles will be reported using the Merchant Contact Information Form, immediately upon changing.

Data Handling

Observe the following data handling requirements:

- Keep cardholder data storage to a minimum by complying with the requirements detailed in the Payment Card Data Handling Procedures.
- Never store the card security code (three-digit or four-digit number printed on the front or back of a payment card).
- Do not store the personal identification number (PIN) or the encrypted PIN block.
- Only the first six and the last four digits of a payment card may be displayed.
- Never send or request card numbers by any end user messaging technologies (e.g. email, voicemail, instant messaging, and text messaging).

Procurement of Payment Systems or Services

Addition of new payment systems or services is considered a change in the University’s payment environment and must follow either the Payment Environment Change Approval Process or the Merchant Account Acquisition Procedure. The CCSP will work with OIT, Procurement Services, and the Merchant to assist in selecting and implementing any new payment system.

Position Changes

For employees with privileged access (i.e., employees with access to more than one instance of cardholder data), merchants must follow the Position Modification Procedure when filling or terminating the position.

Reconciliation and Disputes

Observe the Payment Card Reconciliation Procedures to protect the integrity of fiscal data and to reduce the risk of fraud.

Security Awareness

The Account Owner, Business Manager, and all other individuals who process or have access to cardholder data are required to complete the CCSP Security Awareness Training, upon hire (before handling or having access to cardholder data) and annually. Additionally, these individuals must sign and submit the Policy Attestation Form annually after reviewing all payment card policies.
**System Management**

Observe the following system management requirements:

- Manage all computer systems according to the Technical Standard for Payment Card Processing Systems.
- Limit access to computing resources (e.g., computers, network jacks, wireless access points, gateways, and handheld devices) and cardholder information only to those individuals whose jobs require such access.

**Business Continuity Planning**

It is required that all merchants have a business continuity plan and that they provide that plan to the CCSP office annually. Merchants must be aware that in the case where the CCSP has been breached or in the event of a disaster the environment may be unavailable for a time period no shorter than 48 hours and may be unavailable for a time period greater than one month while investigations are being conducted or recovery efforts are under way. For those merchants that are using third party service providers it is the responsibility of the merchant to be aware of their service provider’s business continuity plan and also to be able to provide that information to the CCSP office.

**Applicability**

This standard applies to all University of Notre Dame employees and students.
Technical Standard for Card Processing Systems

Note: These standards apply to systems in the CCSP environment and virtual terminals.

Computer Requirements

Configuration
All devices must be properly labeled with information that can be correlated to owner and contact information.

Any vendor-supplied defaults (e.g. passwords, SNMP strings, unnecessary accounts) must be changed before connecting any system to the network.

Each system must serve only one primary function and all unnecessary functionality must be removed.

Systems must be configured to meet the applicable Notre Dame security standard as a baseline. In cases where this standard and the Notre Dame standard conflict, this standard takes precedence.

Any non-console administrative access to a system must be encrypted.

Systems commonly affected by malware must have antivirus software installed and configured to log to the central log server. This software must retrieve updates daily.

Personal firewall software must be installed on all Notre Dame owned and maintained computers with direct connectivity to the Internet which are used to access the cardholder data environment.

Only Notre Dame owned and maintained computers are allowed to connect to CCSP environment.

Any changes to system configuration must be completed through the OIT Change Control Process. The change request must include:

- Documentation of impact
- Management approval
- Information Security approval
- Test documentation
- Back-out procedures

System firewalls must be configured to allow only traffic required for documented business purposes.

Authentication
System authentication should use centralized authentication, where possible. Unless documented, the only local account should be an administrator account for emergency use. The password to that account must be stored in the OIT safe in a sealed envelope.

All users must complete an authorization form explicitly approved by management that specifies required privileges. The Assyst RFC System is one tool that may be used to meet this requirement.

All system users must be identified with a unique username and all accounts must be protected by passwords that meet the following requirements (in addition to the University Strong Password Policy Requirements):

- Accounts that are inactive for more than 90 days must be automatically disabled
- No password may be shared by multiple users
- Accounts must be locked out for 30 minutes after six unsuccessful login attempts

Systems must be configured to use a password-protected screen saver after 15 minutes of inactivity.

Passwords must be encrypted during transmission and storage on all system components.

Any remote access to the system must take place through the PCI environment VPN using two-factor (SafeWord) authentication. VPN connection must be immediately deactivated when work is completed. It is prohibited for the copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when remote accessing the PCI environment.

**Monitoring**

The following events must be logged to the central log server:

- Access to cardholder data by an individual
- Actions taken by users with administrative privileges
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Every event logged to the central log server must include the following details:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component or resource

Logs must be reviewed daily with review of all exceptions.

- Audit logs must be retained for one year
- The last three months of audit logs must be immediately available for analysis

All system clocks must be synchronized with the PCI environment’s NTP servers.

Systems must run Tripwire with the policy configured to:

- Ensure that logs may not be altered without generating an alert (new data being added should not generate an alert)
- Alert on any changes to critical files, the modification of which could indicate a system compromise or risk of compromise

Reviews of tripwire reports should be performed weekly with discrepancies being reconciled by OIT- EIS staff.

**Updates**

- Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release. Terminal downloads will be authorized through the Merchant Card Coordinator.
- Follow the Change Control Procedure for all applicable changes.

**Firewall and Network Device Requirements**

**Configuration**

Firewalls and network devices must be configured to meet the applicable Notre Dame security standard as a baseline. In cases where this standard and the other Notre Dame security standards conflict, this standard takes precedence.

Security administrators shall conduct a review of all firewall and router rule sets every six months. (The OIT Information Security staff is responsible for the maintenance, management and configuration of the main CCSP firewalls. OIT Network Services is responsible for the maintenance, management and configuration of network switches, remote site VPN endpoints and the VPN concentrators.)

Firewalls and network devices shall be configured to implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet.

Firewalls will be used at each Internet connection and between any demilitarized zone and the internal network zone. Firewalls shall be configured to:
• Implement a DMZ to filter and screen all traffic and prohibit direct routes for inbound and outbound Internet traffic
• Deny all traffic from untrusted networks and hosts except for protocols necessary for the cardholder data environment
• Restrict inbound Internet traffic to IP addresses within the DMZ
• Not allow internal addresses to pass from the Internet into the DMZ
• Implement stateful inspection
• Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment
• Prohibit direct public access between external networks and any system component that stores cardholder data
• Restrict outbound traffic from payment card applications to IP addresses within the DMZ

Network device configuration files shall be secured and synchronized. Running configuration files and start-up configuration files should have the same secure configuration.

Administrators of firewalls and network devices in the card processing network are responsible for maintaining the following:

• Current network diagram with all connections to cardholder data, including any wireless networks
• Documented list of services and ports necessary for business
• Justification and documentation for any available protocols besides HTTP, SSL, SSH and VPN
• Justification and documentation for any risky protocols allowed (e.g. FTP, telnet) which includes reason for use of protocol and security features implemented

Authentication

Any vendor-supplied defaults (e.g. passwords, SNMP community strings, unnecessary accounts) must be changed before connecting any system to the network.

Each system must serve only one primary function and all unnecessary functionality must be removed.

Any non-console administrative access to a system must be encrypted.

Any external network connections or changes to system configuration must be completed through the OIT Change Control Process. The change request must include:

• Documentation of impact
• Management approval (The Director, Information Security is responsible for approving changes to the Sidewinder firewalls.)
• Information Security approval
System authentication should use centralized authentication, where possible. Unless documented extraordinary circumstances exist, the only local account should be an administrator account for emergency use. The password to that account must be stored in the OIT safe in a sealed envelope.

All system users must be identified with a unique username and all accounts must be protected by passwords that meet the following requirements (in addition to the University Strong Password Policy Requirements):

- Accounts that are inactive for more than 90 days must be automatically disabled
- No password may be shared by multiple users
- Accounts must be locked out for 30 minutes after six unsuccessful login attempts

Passwords must be encrypted during transmission and storage on all system components.

Any remote access to the system must take place through the PCI environment VPN using two-factor (SafeWord) authentication. VPN time out setting must be set to 240 minutes.

**Monitoring**

The following events must be logged to the central log server:

- Access to cardholder data by an individual
- Actions taken by users with administrative privileges
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

Every event logged to the central log server must include the following details:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component or resource

Logs must be reviewed daily with review of all exceptions.

All clocks must be synchronized with the PCI environment’s NTP servers.
Payment Application Requirements
Any payment application that is installed in the Notre Dame Payment Card Environment must be PA-DSS certified and must be implemented in accordance with the vendors implementation guide.

System Defaults
Vendor-supplied defaults must be changed before installing an application system on the network. For instance, change default usernames and passwords and eliminate unnecessary accounts.

System Functions
The server housing the application shall have no unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

System Access
All non-console administrative access to the application must be encrypted. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

Storage of Sensitive Data
Any sensitive data that is stored as a result of the trouble shooting process must be securely deleted at the end of the trouble shooting process.

The application must not be configured to store sensitive authentication data subsequent to authorization (even if encrypted), including:

- The full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.
- The card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions
- The personal identification number (PIN) or the encrypted PIN block.

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the cardholder’s name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.

For applications that display the PAN, user privileges must be varied such that the application must mask the PAN for employees without a specific need to see the full PAN. In such cases, the first six and last four digits are the maximum number of digits to be displayed.
Key Management

Encryption keys Should be managed in accordance with the vendors implementation guide

Security Patches
All system components must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. Patches may be applied using a risk-based approach to prioritize patch installation to ensure high priority systems and devices are addressed within one month, while less critical devices and systems are addressed within three months.

Software Development
In-house developed payment applications are prohibited by the University.

Web Applications
In house hosted web hosting applications are prohibited by the University. Third party hosted web applications must be determined to PCI DSS compliant by the vendor.

Least Privilege
In keeping with the University of Notre Dame Payment Card Business Standard, the application must support limitation of user access to cardholder information only to those individuals whose job requires such access. By default, the application should set access to “deny all” unless specifically allowed.

Authentication and Password Protection
Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Therefore, the application must identify all users with a unique user name before allowing them to access application components or cardholder data. In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password
- Token devices (e.g., SecureID, certificates, or public key)
- Biometrics

The application must require two-factor authentication for remote access by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. Exceptions to this include Bomguard/ WebX support style technologies when used to provide real-time support from approved vendor and the specific implementation is reviewed and approved by the CCSP.
Applications must encrypt all passwords during transmission and storage. In addition, the application and/or application administrator must ensure proper user authentication and password management for non-consumer users and administrators as follows:

- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
- Verify user identity before performing password resets
- Set first-time passwords to a unique value for each user and require change immediately after the first use
- Immediately revoke access for any terminated users
- Remove inactive user accounts at least every 90 days
- Enable accounts used by vendors for remote maintenance only during the time period needed
- Communicate password procedures and policies to all users who have access to cardholder data
- Do not use group, shared, or generic accounts and passwords
- Require change of user passwords at least every 90 days
- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than six attempts
- Set the lockout duration to thirty minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the session
- Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users

**Monitoring**

The application must enable or the application administrator must establish a process for linking all access to application components to each individual user. Automated audit trails are required to reconstruct the following events:

- All individual user accesses to cardholder data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects.

Record at least the following audit trail entries for all system components for each event:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
• Identity or name of affected data, system component, or resource.

In accordance with PCI, audit logs must be maintained for one year, with a minimum of three months immediately available for analysis.

For log integrity, application and/or application server clocks must be synchronized with the NTP server. Further, audit trails must be secured so they cannot be altered. To do so, the application administrator must:

• Limit viewing of audit trails to those with a job-related need
• Protect audit trail files from unauthorized modifications
• Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.
• Copy logs for wireless networks onto a log server on the internal LAN.
• Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

POS “Swipe” terminal Requirements
This standard applies to all land line, IP based and cellular based point-of-sale card processing devices.

Setup
• Always change vendor-supplied defaults before installing a system
• IP based physical terminals must reside on an isolated payment network
• Disable all unnecessary and insecure services and protocols
• Keep cardholder data storage to a minimum; following the prescribed time period and process in the Payment Card Data Handling Procedures.
• Mask the card number when displayed (the first six and last four digits are the maximum number of digits to be displayed). Terminals must be programmed to mask the payment card number on the customer and merchant receipt.
• Password protect all detail reports.
• Follow the Terminal Configuration Procedure for the terminal type in question.

Operations
• Restrict physical access to terminals to authorized users of the terminal. When unattended, terminals must be stored in a locked area.
• Terminals must be settled daily, although they may be settled more frequently. Generate Totals Reports prior to settlement
• Terminals and terminal supplies will be ordered through the campus Merchant Card Coordinator

Wireless and End User Technologies

In accordance with the University of Notre Dame Payment Card Policy, cardholder data will not be transmitted using Wireless Technology, unless specifically approved and
tunneled through a VPN. CHD will not be transmitted via email or other end user technologies.

Anti-Virus, Anti-Adware, and Anti-Spyware Protection
Anti-virus software must be deployed on all systems commonly affected by malicious software (particularly personal computers and servers). Anti-virus programs must be capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware. All anti-virus mechanisms must be kept current, actively running, and capable of generating audit logs.

Virtual Terminal Requirements
This standard applies to standalone as well as VM based virtual terminals. Only PCs running Windows XP or Windows 7 may be used as virtual terminals. All systems must meet the following requirements

Basic System Configuration
- Systems must be joined to the CCSP domain.
- Systems must be connected to the Cardholder data environment through an approved virtual terminal network connection.
- Systems must:
  - receive GPO that applies Tripwire PCI Policy.
  - be connected to EPO for auditing/updating.
  - accept patches via SCCM.
  - configured to log to Q-Radar.
- Auto logon is permissible for virtual terminal end users if access is only to an approved payment applications.

VM based Virtual Terminal Configurations
- End users are restricted to only launching Virtual Machines (VM’s) (productivity and Credit Card VM’s)
- VMware is configured to provide strong isolation between the VM’s.
  - No cutting and pasting between VMs.
  - No file sharing between VMs.
- Separate physical network interface for in scope and out of scope OS’s.
- Host and credit card VMs are in scope and productivity VM is out of scope.
- Auto logon with specifically configured CCSP account is permissible on host.

Payment Network Configurations
- Virtual Terminals will be shielded from the internet by the PCI central firewall through dedicated interfaces.
  - Firewall policy restricts access to approved OIT infrastructure and business partners.
• Distributed using only applicable network hardware.
• Virtual Terminal network jacks are configured to only recognize MAC addresses of approved payment devices.
• Devices must be statically IP’ed with addresses assigned via the approved CCSP RFC process.

Applicability
This policy applies to all University of Notre Dame employees and students.
**Third Party-Vendor Guidelines**

As stated in the University of Notre Dame Payment Card Policy, all Notre Dame merchant activity will be conducted through approved university merchant accounts. However, the University does recognize the need for third party vendors to collect, process, and/or store payment card data on university property. Guidelines for these third party card processing activities are as follows:

- Third party vendors who conduct any card processing activities on campus, whether it be electronically or paper-based, are to comply with the Payment Card Industry Data Security Standard (PCI DSS).
- Vendors may not connect any device to the Notre Dame CCSP Segmented Payment Network for any reason.
- Vendors may connect their electronic card processing devices to the open Notre Dame network, but do so at their own risk. The University will act as an Internet Service Provider (ISP), only offering a direct communication link to the Internet.
- Any exception to these guidelines must be reviewed and approved by the Notre Dame Credit Card Support Program and Information Governance Committee.

**Applicability**

This standard applies to all University of Notre Dame employees or students.
Section 3: University of Notre Dame
Payment Card Processing Procedures
Merchant Account Acquisition Procedures

This procedure specifies actions required of University personnel who wish to accept card payments.

1. A department or unit wishing to accept credit card payments must contact the Credit Card Support Program (CCSP) via email at ccsp@nd.edu, and submit the Payment Acceptance Activity Clarification (PAAC) Form to the CCSP Office.
2. The CCSP will contact the requestor if any further clarification regarding the requested activity is required.
3. The CCSP prepares an Activity Brief which documents the request.
4. The Activity Brief must receive signoff from the requesting department. This includes signatures from the requestor, the department business manager, and responsible university officer.
5. The signed Activity Brief must be returned to the CCSP office in 426 Grace Hall.
6. The Activity Brief will then be forwarded to all members of the Information Governance Committee for a two-week review period.
7. After Information Governance Committee review, the Activity Brief and any comments and/or recommendations from the Information Governance Committee will be discussed with the requesting department and sent to the Vice President for Business Operations and the Vice President for Finance for final approval.
8. If approved by the Officers, the project will transition to the department responsible for implementation of the new merchant activity (e.g. the Merchant Card Coordinator in the Controller’s Office for physical terminals, ND Marketplace for e-commerce, or the OIT for a new IT system).
9. The Merchant Card Coordinator will contact the requesting department to establish a new merchant account and schedule card acceptance and reconciliation training.
10. The CCSP Office provides the account owner with training materials and forms that must be completed prior to account activation.
11. After completion of the project identified in (8), the department or unit is instructed to submit a $1.00 test transaction for each card type prior to activation of the account to verify correct setup. The Merchant Card Coordinator confirms that the transaction reaches the depository bank.
12. The Merchant Card Coordinator completes the merchant account setup by notifying Accounting & Financial Services for posting of revenue and the Tax Department for final review of UBI tax reporting or sales tax requirements.

Applicability

This procedure applies to all University of Notre Dame employees.
Payment Card Data Handling Procedures

In keeping with the Notre Dame Payment Card Policy, storage and disposal of cardholder data must comply with PCI-DSS requirements. In order to meet this policy requirement, departments must limit storage of cardholder data to the amount and time required for business, legal, and/or regulatory purposes.

General Requirements

- The card number must be redacted to not more than the first 6 and/or last 4 digits.
- Do not store the personal identification number (PIN) or the encrypted PIN block.
- Do not store sensitive authentication data subsequent to authorization (even if encrypted.)
- NEVER store the card verification code or value or PIN verification value data elements used to verify card-not-present transactions.
- Electronic storage is prohibited without prior approval obtained through the CCSP.
- Hardcopy records and electronic media containing cardholder data must be inventoried at least annually in order to lessen the chance that the loss or theft of this data goes unnoticed.
- Electronic media containing cardholder data must be disposed of in accordance with PCI (e.g., using "military wipe programs," degaussing, or physical destruction). Contact the University's Information Security department for assistance.
- Retention schedules for documents containing cardholder information are established in partnership with the University Archives' Archivist for Records Management, in accordance with the University’s Records Management and Archives Policy.
- Retention schedules require storage for the minimum length of time required for business, legal, and regulatory purposes.
- Any forms containing cardholder data must be purged of full credit card numbers before they can be sent to the University Archives. The University Archives will not accept any documents containing cardholder data.
- Paper containing payment card data must be disposed of using a cross-cut shredder.

Mail Handling

For cardholder data received via U.S. Mail, always utilize a Business Reply (BR) account.

- For intermittent, low volume activity use the University general account.
- For continuous, high volume activity acquire a departmental BR account.

Note: BR envelopes must meet United States Postal Service (USPS) design specifications and be submitted to the local Post Master for approval.

Have mail containing sensitive cardholder data delivered by Mail Services to a person in the department or to a secure area in the department. Departments picking up their own Post Office Box mail should maintain physical control of mail until delivered to a person or secure area in the department.
BR mail is counted and bundled by the USPS. Confirm the number of items received in each days bundle to the USPS count and compare the monthly volume to the volume in that month’s bill.

Any department wishing to receive cardholder data via physical mail without a BR account must request an exception to policy using the Payment Acceptance Activity Clarification Form. The request must include a description of the alternate process whereby receipt of cardholder data will be tracked. Contact the CCSP office to do so.

Receipt of cardholder data via end-user messaging technologies (e.g. email, voicemail, instant messaging, and text messaging) is disallowed.

**Chargeback Handling**  
The Merchant Card Coordinator (MCC) will receive all Chargeback Summary, Chargeback Notification, or Request for Transaction Documentation forms from the University’s merchant bank. The MCC will make all cardholder numbers unreadable on the Chargeback Summary, Chargeback Notification or Request for Transaction Documentation.

Two (2) copies of the form(s) will be made.

- One copy is retained in the MCC’s file.
- One copy is sent to the Merchant Account Owner for handling.
- The original document(s) will be cross cut shredded by the MCC.

Note: The Merchant Card Coordinator can utilize My Merchant View should the Merchant Account Owner need a card number for research.

**Applicability**

This procedure applies to all University of Notre Dame employees.
Payment Card Reconciliation Procedures

Reconciliation of credit card sales is the responsibility of the Business Manager or the account owner where delegated. Regular reconciliation insures deposits are accurate and timely. We recommend that reconciliations occur weekly, but at a minimum, monthly.

We have provided you with an example of a monthly reconciliation to demonstrate how easy it is to create an excel spreadsheet, list daily sales, and reconcile to the general ledger.

A few items to remember:

1. MasterCard/Visa/DiscoverCard sales are combined and funded as one deposit. American Express & DiscoverCard are each funded separately.
2. Generally, MasterCard/Visa/DiscoverCard combines Friday, Saturday, and Sunday sales and funds them as one deposit. In our example you can see that Friday, November 7th, Saturday, November 8th, and Sunday, November 9th were received on Wednesday, November 12th. American Express may combine batches, although there is no consistent pattern. Your spreadsheet will help you determine which days are combined and posted as one amount on the general ledger.
3. MasterCard/Visa/DiscoverCard sales are generally funded within two (2) business days of the settlement date. American Express sales are generally funded within three (3) days of the settlement date.
4. Our example is for the month of November only. There are timing differences where late October sales are received and posted in early November and late November sales are received and posted in early December. Your spreadsheet will be an ongoing list of sales, making it easy to see timing differences.

Note: Letters have been superimposed onto the spreadsheet of daily credit card activity and the Touchnet batch settlement report to show relationships between the two. Additionally, numbers have been superimposed on the daily credit card activity and the general ledger reports to show the relationships between the two.

Procedure:

1. Create an Excel spreadsheet to input daily credit card activity.
2. Column headings would be: DATE  MC-VISA-DISC  AMEX  TOTAL.
3. For each day list credit card sales by card type using TouchNet Batch Settlement report or application report or credit card terminal batch settlement report as source documents, depending on your payment gateway. A TouchNet account is used in this example.
4. Daily batch totals from the source document and daily spreadsheet totals should equal for each day.

5. Depending on where you have requested credit card revenue to be posted, pull General Ledger reports for the reconciling period from *Self-Service Banner, GL-ez, or Asset & Liability* reports.

<table>
<thead>
<tr>
<th>Transaction Date</th>
<th>Activity Date</th>
<th>Document Code</th>
<th>Vendor/Transaction Description</th>
<th>Amount</th>
<th>Rule Class Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-Nov-08</td>
<td>10-Nov-08</td>
<td>MC001210</td>
<td>11/3 Credit Card Revenue</td>
<td>28.49</td>
<td>FC1</td>
</tr>
<tr>
<td>4-Nov-08</td>
<td>10-Nov-08</td>
<td>MC001211</td>
<td>11/4 Credit Card Revenue</td>
<td>293.00</td>
<td>FC1</td>
</tr>
<tr>
<td>5-Nov-08</td>
<td>10-Nov-08</td>
<td>MC001212</td>
<td>11/5 Credit Card Revenue</td>
<td>1,474.50</td>
<td>FC1</td>
</tr>
<tr>
<td>6-Nov-08</td>
<td>10-Nov-08</td>
<td>MC001213</td>
<td>11/6 Credit Card Revenue</td>
<td>204.50</td>
<td>FC1</td>
</tr>
<tr>
<td>7-Nov-08</td>
<td>10-Nov-08</td>
<td>MC001214</td>
<td>11/7 Credit Card Revenue</td>
<td>204.50</td>
<td>FC1</td>
</tr>
<tr>
<td>10-Nov-08</td>
<td>17-Nov-08</td>
<td>MC001216</td>
<td>11/10 Credit Card Revenue</td>
<td>20.00</td>
<td>FC1</td>
</tr>
<tr>
<td>10-Nov-08</td>
<td>17-Nov-08</td>
<td>MC001216</td>
<td>11/10 Amer Expr Revenue</td>
<td>122.75</td>
<td>FC1</td>
</tr>
<tr>
<td>12-Nov-08</td>
<td>17-Nov-08</td>
<td>MC001217</td>
<td>11/12 Credit Card Revenue</td>
<td>315.99</td>
<td>FC1</td>
</tr>
<tr>
<td>13-Nov-08</td>
<td>17-Nov-08</td>
<td>MC001218</td>
<td>11/13 Credit Card Revenue</td>
<td>26.42</td>
<td>FC1</td>
</tr>
<tr>
<td>17-Nov-08</td>
<td>24-Nov-08</td>
<td>MC001221</td>
<td>11/17 Amer Expr Revenue</td>
<td>264.75</td>
<td>FC1</td>
</tr>
</tbody>
</table>

Report Total (of all records): 2,954.90

6. Compare General Ledger postings to spreadsheet to insure all sales have been received and posted to the General Ledger.

7. If there is a discrepancy or you need assistance, please feel free to call the Merchant Card Coordinator.

**Applicability**

This procedure applies to all University of Notre Dame employees.
Payment Environment Change Approval Procedure

This procedure specifies actions required of departments that wish to change their existing payment environment, including but not limited to:

- The re-purposing of existing merchant accounts
- The alteration of payment systems
- Any change in business process that affects how card data is processed or handled
- The addition of or change to any connections to the CCSP Segmented Payment Environment
- The addition or alteration of relationships with third-party payment service providers.

1. Any department or unit wishing to make any change to their payment environment as outlined above must contact the Credit Card Support Program (CCSP) and submit the Payment Acceptance Activity Clarification (PAAC) Form to the CCSP Office.
2. The CCSP will contact the requestor if any further clarification regarding the requested change is required.
3. After a preliminary review with the Information Governance Committee, the requested change will be classified as either “minor” or “significant”.
   3.1. A MINOR change is one that does not significantly change the process, technology, or risk associated with the merchant’s payment acceptance activity.
   3.1.1. Minor changes will be reviewed and either accepted or rejected directly by the Information Governance Committee. The CCSP Office will inform the requesting department of the Information Governance Committee’s decision within 1 week of the request date.
   3.2. A SIGNIFICANT change is one that would cause the merchant’s payment acceptance activity to change in such a way that the risks associated with it need to be formally re-assessed by the Information Governance Committee and approved by University officers. Specifically, significant changes require approval from the Vice Presidents of Business Operations and Finance. To facilitate this:
   3.2.1. The CCSP will prepare a formal Activity Brief which documents the request.
   3.2.2. The Activity Brief must first receive signoff from the requesting department. This includes signatures from the requester, the department business manager, and responsible university officer.
   3.2.3. The signed Activity Brief must be returned to the CCSP office in 426 Grace Hall.
   3.2.4. After Information Governance Committee review, the Activity Brief and any comments and/or recommendations from the Information Governance Committee are reviewed with the requesting department (within three weeks of the request date) and then sent to the Vice President for Business Operations and the Vice President for Finance for final approval.
4. If the requested change is approved by the Officers, the CCSP group will work with the merchant (or requestor) to implement the change as described in the request.
Position Modification Procedure

Identification of Positions with Privileged Access
In fulfillment of Payment Card Industry Data Security Standard requirements, positions with access to multiple instances of cardholder data are identified using the Registry of Positions with Privileged Access. Each merchant account owner must keep their registry up-to-date. Each merchant will provide their registry to the CCSP annually and on request. The CCSP will then compile a master registry for use by the Office of Human Resources (HR) in tracking changes to positions with Privileged Access.

Modification of Positions with Privileged Access
Privileged Access will be provided only to employees with a functional need for such access, in accordance with the University’s Data Access Policy. When a position with Privileged Access is created or discontinued and when Privileged Access is added to or withdrawn from an existing position:
1. The merchant will include the level of access in the Position Description.
2. The merchant will notify HR of the change.
3. The merchant will indicate the access level of the position on HR forms where requested.

Hiring
When filling a position with Privileged Access, merchants will notify the CCSP using the Merchant Contact Information Form prior to the employee starting

External Candidates
A criminal background check will be run for all external applicants to positions with Privileged Access. Candidates whose backgrounds contain a financial infraction within the last seven years are deemed ineligible for the position now and in the future. Depending upon the totality of background information, the candidate may be ineligible for other employment for at least six months.

Internal Transfers
Except where a criminal background check occurred within the preceding twelve month period, a criminal background check will be run for all internal applicants to positions with Privileged Access. Candidates whose backgrounds contain a financial infraction within the last seven years are deemed ineligible for the position now and in the future.

Separation
Upon separation of an employee with Privileged Access:
1. Merchants will notify the CCSP using the Merchant Contact Information Form.
2. The merchant will revoke access to cardholder information, immediately upon separation.
Credit Checks
HR will use discretion to conduct a credit check only if conviction information on background check suggests possible financial misdeeds that a credit check might shed further light on.

Applicability
This procedure applies to Notre Dame employees who supervise or hold positions with Privileged Access. Privileged Access refers to the ability to access multiple instances of cardholder data at one time. Examples of positions with Privileged Access include Database Administrators of payment application databases where cardholder data are stored, staff with access to multiple paper forms containing cardholder information, and terminal operators with the ability to run batch reports containing cardholder information. An example of a position with non-privileged access to cardholder data is a cashier, handling one transaction at a time.
**CCSP Database Update Procedure**

**Purpose:**

To ensure that as changes are made to the CCSP Payment Environment they are updated appropriately in the CCSP Database. The Assyst RFC System will be the vehicle in which changes are communicated through. The outline below describes what area will be responsible for making updates to the Device table within the CCSP database. The overall idea is that when changes are made to regarding networking or O&E that they are responsible for updating those changes to the device table with the CCSP database. All additions of new devices or removal of devices will be made by the CCSP Office. In addition all users should utilize the notes section to capture the RFC number(s) associated with the change as well as note the date and person and who made the last change.

**Networking:**

Any networking changes within the CCSP environment will be update by Networking. Requests from merchants to swap physical terminals and/or virtual terminals locations will be handled by Networking and will be updated appropriately. Specifically when changes to the network configuration for physical terminals, virtual terminals, switches, and jacks are requested Networking will be responsible for updating the following fields within the device table (IP Address, Vlan, Jack, Port, Switch, MAC Address, and building location if necessary).

**Enterprise Infrastructure Services:**

Any changes to servers located within the payment environment will be updated by Operations and Engineering when they occur. Software version updates to servers will also be recorded by O&E when they occur. Specific fields within the device table will be the responsibility of O&E when server changes are made (DNS Name, IP Address, and Software Version).

**CCSP Office:**

The CCSP office will be responsible for entering all new information pertaining to merchant account activity, physical terminals, virtual terminals, servers, and switches. The CCSP office will also be responsible for removing servers, virtual terminals, physical terminal, and switches from the device table when they are removed from the environment.

**Applicability**

This procedures policy applies to all University of Notre Dame employees and students.
Section 4: Payment Acceptance Options
E-Commerce: The Notre Dame Marketplace

Overview

The ND Marketplace provides campus organizations with a secure and cost-effective way to extend their business operations to the World Wide Web. The service supports a wide variety of e-commerce needs including:

- the sale of merchandise
- the sale of publication subscriptions
- event registration
- donations acceptance

Services

Store Design and Implementation: E-commerce sites are designed and built with the merchant’s unique business requirements and design preferences in mind. The five step design process ensures that merchants get the most out of their e-business.

Technical Support: All technical support is free. If at any time a merchant has a question about their store, ND Marketplace staff is on hand to help.

Consulting Services: In addition to ensuring that online businesses meet all government and university requirements and follows industry best practices, the ND Marketplace is also committed to helping merchants continually improve their online store in terms of customer satisfaction and back office efficiency. The ND Marketplace provides custom reporting capabilities, and offers a number of Search Engine Marketing and Optimization (SEM and SEO) services.

Merchant Options

To suit the needs of campus merchants, the Marketplace offers two distinct options, uStores and uPay:

- **uStores** is the full service ecommerce option; the Marketplace will build and host your entire ecommerce website, including, product pages, shopping cart, checkout pages, and reports.
- **uPay** provides a way for merchants to connect a secure checkout process to their existing website or application. In short, merchants add a “Pay Now” button to their website, and customers are redirected to complete their transaction securely and efficiently.

For More Information on Services, Stores, or to Request a Store, please visit [http://marketplace.nd.edu](http://marketplace.nd.edu), or call 1-2991.
Card Present & Mail Order/Telephone Order (MOTO) Transactions

ExaDigm Card Swipe Terminals

Overview

The CCSP has selected two types of credit card terminals to facilitate acceptance of card present, mail order, and telephone order transactions. These terminals were selected for campus use because they encrypt card holder data during transmission and while being stored in the terminal prior to settlement. Both customer and merchant receipts mask the cardholder number allowing us to further protect cardholder data. Terminals are requested through the CCSP office. Merchants are responsible for the purchase price of the terminal and monthly cellular service charges, if applicable.

Types of Swipe Terminals

The XD1000 is a countertop point of sale device that connects to the university’s segmented payment environment through an IP connection. Once installed these terminals must remain connected through the designated IP connection and cannot be moved without the approval of the CCSP. IP based transactions are faster and therefore the preferred method of communication with our processor.

The XD2100 is a mobile point of sale device utilized when a wired connection is not feasible. These terminals connect to our processor via a cellular connection. If the XD2100 is chosen as the terminal of choice, the Merchant Card Coordinator works with the Telecommunications Department to establish data cellular service. Monthly charges vary depending on the number of transactions and are billed directly to the merchant’s FOAPAL.
**Virtual Terminals**

**Overview**

A Virtual terminal is any personal computer that is used by an employee to enter customer credit card data directly into a payment gateway or other website. Virtual terminals are alternatives to physical card-swipe terminals such as Exadigm, but are typically not preferable because of the added costs and security requirements associated with them. Explicit approval is needed before any personal computer is used as a virtual terminal.

**When is use of a Virtual Terminal Appropriate?**

There are situations where a virtual terminal is a necessary alternative to a physical terminal. Typically, these are situations where advanced reporting capabilities are required by the merchant. Physical terminals have a small ticker tape printer that can print receipts and limited reports for the merchant, but cannot be used to download any data to a excel file or the equivalent. In situations where this type of data retention is absolutely required, a virtual terminal might be necessary.

**Security Requirements**

In order to ensure that cardholder data is protected and PCI DSS requirements are met, virtual terminals must be maintained to a higher security standard than all other university computers. Every year, an assessment will need to be done on each virtual terminal, to verify that the proper security settings are applied to the machine. The department’s IT contact, whether they are associated with OIT DSS support or otherwise, is responsible for completing the assessment on their own. Having that expertise to complete the assessment is a requirement for departments that are requesting use of a virtual terminal.
Other Payment Acceptance Options: Custom OIT/Procurement Projects

Overview

If the standard payment acceptance options do not meet the unique needs of your department, it would be necessary at that point to begin a project with OIT and Procurement Services to find a solution. Examples of custom payment acceptance methods currently in use at the university include the Paciolan ticketing system and the NDFS Micros cash register network.

Depending on the specifics of your request, a formal OIT project and or a Request for Information / Request for Proposal generated through Procurement Services might be required. Long lead times are typically required for each of these processes, so please plan ahead when considering any custom payment acceptance options. The CCSP can help you determine if a custom project is necessary, or if an existing campus solution could work for you.
Mobile Payment App

Overview

Transform your mobile phone into a point-of-sale (POS) device and process payments whenever and wherever you are. Fast and simple, the e-Select plus Mobile App allows you to accept payments and close sales on the spot.

Available for use on many smartphones, the e-Select plus Mobile App features real-time authorization, emailing of receipts, and reporting to help maximize your business efficiency and cash flow.

Flexibility and Convenience

- Multiple users can download the app and process transactions at the same time
- Moneris mobile card reader simply plugs into the audio port of your smartphone

Faster and Easier Sales

- Capture sales on the spot for services rendered or products sold
- Payment receipt can be emailed directly to your customer

Cost Savings

- Every time you swipe a card you may qualify for a lower rate per transaction

Security

- Card data is encrypted at the time of swipe and transmitted over SSL for extra security
- No customers’ data is retained on your mobile phone

Real-time Reporting

- Check transaction history and reports on your smartphone or online anytime
- User based reporting allows you to monitor transactions by independent users
Section 5: CCSP Forms
After completing the form, please save it for your records. Upon request, please email it to the CCSP Office.

```
<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Net ID</th>
<th>Address 1</th>
<th>Address 2</th>
<th>City</th>
<th>State</th>
<th>Zip</th>
<th>Email</th>
<th>Phone</th>
<th>Privileged Access</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
After completing the form, please save it for your records. Upon request, please email it to the CCSP Office. (An up-to-date form will be requested annually.)

<table>
<thead>
<tr>
<th>SerialNumber</th>
<th>Hostname</th>
<th>DNSName</th>
<th>IPAddress</th>
<th>MACAddress</th>
<th>OperatingSystem</th>
<th>Machine Type or Device Model</th>
<th>Department</th>
<th>Owner Name</th>
<th>Admin Name</th>
<th>Building</th>
<th>Rm #</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version 2007.04.09(2)
CCSP Business Continuity Plan

Merchant Account DBA: ______________________
Merchant ID: ______________________

Scope and Objective
This Business Continuity Plan documents this merchant’s response to an unplanned outage to their standard card processing capabilities, either due to a suspected data compromise or other unplanned event.

Business Continuity Coordinator:
BCC Contact Information: Telephone –
Cell Phone –
e-mail –

Date Plan Updated:
Plan Updated By:

Page 1 of 2
# Payment Acceptance Activity Clarification Form

## Contact Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Name</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>Office or Department</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>Phone</td>
<td>Click here to enter text.</td>
</tr>
<tr>
<td>Fax</td>
<td>Click here to enter text.</td>
</tr>
</tbody>
</table>

## Purpose of Document

1. Please indicate the purpose of this document:

   - [ ] Documentation of a new payment acceptance process
   - [ ] Documentation of an existing payment acceptance process
   - [ ] Request to change a previously approved Payment Acceptance Process
   - [ ] Other: Click here to enter text.

## Overview of Activity

2. Please provide an overview of the current or proposed activity to be reviewed. Please include its purpose, a detailed description of the business process, a list of outside vendors and/or software that are or may be involved with this process, and any other information you deem appropriate.

   Click here to enter text.

## Payment System

3. Please describe the payment system involved/proposed (Web-based, terminal, 3rd party software, manual handling of cards or card data, etc.). Include model numbers for known equipment and version numbers for software.

   Click here to enter text.

## Sensitive Data

4. If this is an existing activity, is sensitive cardholder data (more than the first and last four digits, card validation codes, or magnetic stripe data) stored in any format (paper or electronic)? If so, under what circumstances (be specific).

   Click here to enter text.

## Time Constraints

5. Are there any time constraints on the implementation or review of this activity that stakeholders need to be aware of?

   Click here to enter text.

## Sign-Offs

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestor</td>
<td>[CLICK HERE TO TYPE NAME]</td>
</tr>
<tr>
<td>Date</td>
<td>Click here to enter a date.</td>
</tr>
</tbody>
</table>
**Business Process Form Assessment**

**Merchant Account Name:**

**Name of Assessor:**

**Date of Assessment:**

**Account Owner:**

**Business Manager:**

**Director:**

**IT Contact:**

**List of facilities and locations where Merchant account is used:**

<table>
<thead>
<tr>
<th>(PCI DSS Req.)</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>1</td>
<td>While conducting business under this merchant account, do you or does anyone in your department come into contact with full credit card numbers or other cardholder data (e.g. security codes)? This applies to ANY and ALL activity that is associated with this Merchant ID.</td>
</tr>
<tr>
<td>IF YOU ANSWERED NO TO QUESTION 1, YOU MAY SKIP AHEAD TO QUESTION 7.</td>
<td></td>
</tr>
<tr>
<td>(7.1)</td>
<td>2</td>
</tr>
<tr>
<td>(4.2)</td>
<td>3</td>
</tr>
<tr>
<td>(9.1.2)</td>
<td>4</td>
</tr>
<tr>
<td>(9.1.3)</td>
<td>5</td>
</tr>
<tr>
<td>(9.7.2)</td>
<td>6</td>
</tr>
<tr>
<td>a</td>
<td>If yes, is the cardholder data sent via Business Reply Mail?</td>
</tr>
<tr>
<td>b</td>
<td>Otherwise, please describe how cardholder data is sent via mail:</td>
</tr>
<tr>
<td>9.6</td>
<td>7</td>
</tr>
<tr>
<td>(9.7)</td>
<td>a</td>
</tr>
<tr>
<td>(9.7.1)</td>
<td>b</td>
</tr>
<tr>
<td>(9.9)</td>
<td>c</td>
</tr>
<tr>
<td>d</td>
<td>Do any employees take or send paper or electronic media containing full credit card numbers off site.</td>
</tr>
<tr>
<td>(9.10)</td>
<td>e</td>
</tr>
<tr>
<td>(3.1)</td>
<td>f</td>
</tr>
<tr>
<td>(12.6)</td>
<td>8</td>
</tr>
<tr>
<td>(12.1)</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>Has the account owner reviewed the original activity brief for this merchant account and validates that the card processing method has not changed?</td>
</tr>
<tr>
<td>(12.9.1)</td>
<td>11</td>
</tr>
</tbody>
</table>

**Assessor's Signature**

With my signature I confirm that this assessment accurately describes all activities associated with the merchant account listed above.

X__________________________

Signature Date

http://ccsp.nd.edu

CCSP Merchant Manual v1.09 Page 67
**Policy Attestation Form**

<table>
<thead>
<tr>
<th>Payment Card Industry - Data Security Standard (PCI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Attestation</td>
</tr>
</tbody>
</table>

Credit Card Support Program (CCSP)
426 Grace Hall
Notre Dame, IN

<table>
<thead>
<tr>
<th>Department:</th>
<th>DBA:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MID:</th>
<th>Account Owner:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Director:</th>
<th>IT Contact:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I have read and understand the Universities security policies published on the following websites:

- [http://ccsp.nd.edu/policy/policy.shtml](http://ccsp.nd.edu/policy/policy.shtml)
- [http://ccsp.nd.edu/policy/paymentCardPolicy.shtml](http://ccsp.nd.edu/policy/paymentCardPolicy.shtml)

<table>
<thead>
<tr>
<th>Last Name:</th>
<th>First Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Net ID:</th>
<th>Privileged Access: * (YES/NO)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Signature:  

Date:  

Affirmation that you have reviewed these policies and procedures satisfies 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."

*Positions with Privileged Access are those positions providing access to multiple instances of sensitive cardholder data at any point in time. Thus, a cashier position, which affords access to one card number at a time, would not be included. A position that provides access to a report containing a summary report with multiple card numbers would be included.*

Instructions:
1. Provide a certification form for each person who processes credit card transactions for this account.
2. Update Account Owner, Director, or IT Contact with changes (if necessary).
3. Return completed forms to the CCSP Office at 426 Grace (attn: Ryan Palmer).
4. Contact Jeff Simko (1-2639), Lisa Kresnak (1-9947) or Ryan Palmer (1-3503) with questions.
### Service Provider Functional Assessment Checklist

<table>
<thead>
<tr>
<th>Test Requirement</th>
<th>Testing Procedure</th>
<th>In Place</th>
<th>Not In Place</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify that the contract between the University and the Service Provider includes an acknowledgement by the service provider of their responsibility for securing cardholder data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have a program in place to monitor the service provider's PCI DSS compliance status? (This can be accomplished by verifying that the service provider is included in this list on Visa's website (<a href="http://usa.visa.com/download/merchants/cisp-list-of-pciss-compliant-service-providers.pdf">http://usa.visa.com/download/merchants/cisp-list-of-pciss-compliant-service-providers.pdf</a>), or alternatively, asking your service provider for proof that they’ve been successfully validated as a PCI compliant service provider within the past year.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Assessor’s Signature**

With my signature I confirm that this assessment accurately describes all activities associated with the merchant account listed above.

X __________________________ Date __________________________

Signature __________________________
NOTICE REGARDING
PAYMENT CARD INDUSTRY SECURITY
BACKGROUND CHECK

IMPORTANT - PLEASE READ CAREFULLY BEFORE SIGNING AUTHORIZATION

The University of Notre Dame (“the University”) intends to comply with the Payment Card Industry Data Security Standard that requires a background check for all employees with “privileged access”. Your current position is deemed to have “privileged access” to cardholder data, and is included in the requirement. The background information obtained will include a criminal history record. Under certain circumstances (such as if you are suspected of theft and/or fraud related to your employment, or if you are applying for or being considered for a promotion or change of assignment), the University may conduct an additional background check during the course of your employment. Upon your execution of the following Authorization, the University may obtain certain background information from an outside agency.

If the University intends to use any information obtained through this background check in whole or in part in making an adverse employment decision, the University will provide you with (1) a copy of your background report and (2) a written summary of your rights under the Fair Credit Reporting Act before making the adverse decision.

AUTHORIZATION

I acknowledge receipt of the NOTICE REGARDING PAYMENT CARD INDUSTRY SECURITY BACKGROUND CHECK (“the NOTICE”), and certify that I have read and understand the NOTICE and this Authorization. I hereby authorize the University of Notre Dame to obtain background information about me from an outside agency for purposes of evaluating any aspect of my current employment and/or my future employment with the University.

_________________________________________  __________________________
SIGNATURE                                           DATE

_________________________________________  __________________________
PRINTED NAME                                        SOCIAL SECURITY NUMBER

_________________________________________  __________________________
ADDRESS                                               DATE OF BIRTH

_________________________________________  __________________________
CITY, STATE, ZIPCODE                                COUNTRY OF RESIDENCE

_________________________________________
DEPARTMENT/FOAPAL
### Quarterly Network Inspection Worksheet

<table>
<thead>
<tr>
<th>Assessor: Enter name here</th>
<th>Date: Enter date here</th>
<th>Result: Enter PASS or FAIL here</th>
</tr>
</thead>
</table>

#### PURPOSE:
The purpose of this assessment is two-fold:
1. To meet PC/RC/SS Requirement 11.1, which requires us to check for rogue wireless access points quarterly.
2. To follow many of the recommendations published in the PCI Council’s Slimming Invention Document. By visually inspecting POS devices, we can minimize the risk of tampering, and help ensure that cardholder data is not compromised by the POS device itself.

#### INSTRUCTIONS:
During this inventory, you'll be asked to perform the following:
1. Record the CCSP jack numbers, and verify via visual inspection that only approved devices are attached.
2. Record any other device (POS, VT) serial numbers, and perform a visual inspection to verify that the device does not appear to have been opened or tampered with, and that there is nothing else plugged into it other than a network cable and power cord.
3. Verify that the cable connected to the jack appears to be the original cable installed by the CCSP or OIT.
4. Verify that there are no CCSP labels affixed to all network components.

<table>
<thead>
<tr>
<th>Serial/Jack #</th>
<th>Type of Component (POS, VT, other)</th>
<th>Are there any approved devices connected?</th>
<th>Based on a visual inspection, does the device appear to have been opened or tampered with?</th>
</tr>
</thead>
</table>
Sample Email Response

Dear (Insert Name),

Please be aware that without encryption, email is a non-secure method for transmitting information. Therefore, it is against University policy to collect credit card information via email. In order to best protect your personal data and to adhere to industry’s credit card standard, I have deleted your card number in this reply, and unfortunately cannot process your payment unless your credit card is submitted through our secure system.

Thank you,
(your name)
Section 6: Frequently Asked Questions

(For the most recent version of this FAQ, please visit http://ccsp.nd.edu)
Q. Who is responsible for ensuring that all CCSP related documentation is filled out?

A. The Account Owner is ultimately responsible for all assessments and documentation related to their merchant account. Although other personnel and resources might be necessary to complete some of the assessments that the department receives from the CCSP, it is the account owner’s responsibility to coordinate those resources to complete the assessments in a timely manner.

Q. When are my assessments due?

A. Assessments are due once per year. The exact timing depends on your department. The CCSP Office will always send a reminder email at least one month in advance of the assessment due date. Contact the CCSP Office for details about your assessment schedules.

Q. Where can I find the CCSP training material set forth in the Business Process Assessment?


Q. Who needs to complete the CCSP Online Training?

A. Account contacts, including the account owner and business manager, as well as any employee who has access to cardholder data must complete the online training. Each individual must complete the training at least once per year.

Q. What CCSP training modules apply to my merchant account?

A. The training modules are not merchant account specific. Rather, they are job position specific. For example, if your merchant account is tied to a card-swipe terminal, then the account owner would take the account owner training, while other “cashiers” would take the training module specific to card-swipe terminals. The account owner training encompasses everything in the three other training modules, since the account owner needs to be familiar with all card processing policies and procedures.

Q. Who must sign the Policy Attestation Form?

A. The Account Owner, IT Contact and Business Managers must sign the form. Additionally, anyone else that may come into contact with credit card information within your department also needs to review the policies and sign the form.

Q. What are the requirements for using a Virtual Terminal?

A. If a merchant elects to use utilize a virtual terminal they must first submit the request to the CCSP Office. Once approved, the virtual terminals must be implemented and configured in
accordance with CCSP requirements. This includes using predefined CCSP desktop images and GPO’s, connecting to the specified CCSP Network, and installing ePO and Tripwire reporting tools to facilitate the assessment of these systems. The department’s IT Contact must ensure that virtual terminals are properly configured and reporting to the CCSP’s centralized reporting tools.

Q. What CCSP/PCI requirements apply to prospective university vendors and service providers?

A. All university service providers must be validated as either a Level 1 or Level 2 PCI Compliant service provider. Additionally, the service provider must be willing to state in writing that they will be responsible for the credit card data that they possess on our behalf.

Payment applications must be PA-DSS validated.
Section 7: Glossary
**Account number:** Payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Primary Account Number (PAN).

**Application:** Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications.

**Authentication:** Process of verifying identity of a subject or process.

**Authorization:** A process by which a card issuer approves a transaction for a specified amount with a merchant.

**Card Validation Value or Code:** Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand:

- CAV Card Authentication Value (JCB payment cards)
- CVC Card Validation Code (MasterCard payment cards)
- CVV Card Verification Value (Visa and Discover payment cards)
- CSC Card Security Code (American Express)

Note: The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:

- CID Card Identification Number (American Express and Discover payment cards)
- CAV2 Card Authentication Value 2 (JCB payment cards)
- CVC2 Card Validation Code 2 (MasterCard payment cards)
- CVV2 Card Verification Value 2 (Visa payment cards)

**Cardholder:** Customer to whom a card is issued or individual authorized to use the card. The person or entity whose name is embossed on the face of the card.

**Cardholder data:** As defined by the PCI Security Standards Council, consists of the Primary Account Number alone, and also includes the Cardholder Name, Service Code, and Expiration Date when any of these elements are stored in conjunction with the PAN.

**Cardholder data environment:** Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.
**Chargeback**: is a reversal of a payment card transaction initiated by the consumer who holds the card or the bank that issued the card used in the purchase.

**Chargeback Notification**: This is the official notice for a chargeback. The notice provides sales information and a deadline for a response. There is a $9.00 fee from the Merchant Bank for this notice regardless of resolution.

**Chargeback Summary Service Code**: Provides a status report of Chargebacks issued to the Merchant. No response is required.

**Credit card**: Payment method that allows the cardholder to make payments for goods and services and receive cash through credit for the card-issuing bank.

**Charge card**: A credit card which requires payment in full upon receipt of the statement.

**Compensating controls**: Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

**Data Compromise**: Also referred to as a breach. Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.

**Debit card**: Payment method that allows the cardholder to make payments through direct withdrawal from the cardholder’s bank account.

**Default password**: Password on system administration or service accounts when system is shipped from the manufacturer; usually associated with default account. Default accounts and passwords are published and well known.

**Encryption**: Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

**Firewall**: Hardware, software, or both that protect resources of one network from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.

**Hosting Provider**: Offer various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of “shopping cart” options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server.
**Magnetic Stripe Data (Track Data):** Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business.

**Merchant:** Any University entity that participates in card processing activities.

**Merchant account:** An account established by contractual agreement between a merchant/business and a bank or payment gateway.

**Merchant Card Coordinator:** University position that serves as the interface between the merchant bank and merchants. The Merchant Card Coordinator provides support, training, and general service to merchants in all areas relating to payment card processing (e.g., reconciliation, disputes, compliance).

**Payment cards:** Credit cards, debit cards, and charge cards issued by a financial institution.

**Payment gateway:** An e-commerce application service provider service that authorizes payments for e-businesses, online retailers, bricks and clicks, or traditional brick and mortar. It is the equivalent of a physical point of sale terminal located in most retail outlets. Payment gateways encrypt sensitive information, such as credit card numbers, to ensure that information passes securely between the customer and the merchant.

**Point to Point Encryption (P2PE):** A point – to – point encryption (P2PE) solution is provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider’s secure decryption environment.

**Primary Account Number:** Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number.

**Privileged Access:** Access to more than one card number at a time, as opposed to access to a single card number for purposes of completing a transaction (Thus, the term describes positions such as database administrators of systems that house cardholder data, but not cashiers handling one card at a time).

**Request for Transaction Documentation:** Customer does not recognize the transaction and requests additional information from the merchant such as a signed sales receipt. Notice will have a deadline for response. Customer still has the option of disputing the transaction with a Chargeback Notification then being issued. There is no charge for this request from the Merchant Bank.
**Sensitive Authentication Data:** Data that may not be retained subsequent to the merchant receiving the initial authorization response message. Consists of:

- Card Validation Code 2
- Track 1 or Track 2 from the Magnetic Stripe
- PIN Blocks

**Service Provider:** Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

**SAQ:** Acronym for “Self-Assessment Questionnaire.” Tool used by any entity to validate its own compliance with the PCI DSS.

**Skimming:** Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant. The thief can procure a victim’s credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim’s credit card numbers.

**SQL injection:** Form of attack on database-driven web site. An attacker executes unauthorized SQL commands by taking advantage of insecure code on system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database.

**Token:** Device that performs dynamic authentication

**Two-factor authentication:** Authentication that requires users to produce two credentials to access a system. Credentials consist of something the user has in their possession (for example, smartcards or hardware tokens) and something they know for example, a password). To access a system, the user must produce both factors.

**Virtual Terminal:** Allows merchants who have internet access to take orders over the phone or mail and manually enter credit card information without the need for an internet storefront.

**Wireless Technology:** Includes any technology used to transmit data without a physical connection.

**XSS:** Cross-site scripting. Type of security vulnerability typically found in web applications. Can be used by an attacker to gain elevated privilege to sensitive page content, session cookies, and variety of other objects.
Section 8: Training
The University provides security awareness training to those individuals that handle highly sensitive information (HSI) as part of their normal job function. In order to complete the mandatory training you must contact Ryan Palmer atrpalmer3@nd.edu in order to obtain an account to the online training. Once you have been granted an account you will be sent a welcome email with detailed instructions on how to activate your new account. If you have any questions regarding any of the training material or general questions please contact Ryan Palmer.

If you already have been granted an account please follow the link below to access your account.

https://nd.securingthehuman.org/ca_main.php
Section 9: External Resources
Links have been provided to various PCI related websites that provide further information related to PCI DSS.

**PCI Security Standards Council**
https://www.pcisecuritystandards.org/

**Treasury Institute for Higher Education**
http://treasuryinstitutepcidss.blogspot.com/

**PA-DSS List of Validated Payment Applications**
https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html

**Visa's List of Compliant Level 1 Service Providers**