University of Dayton
Credit / Debit Card Acceptance Policy
September 1, 2009

Effective Date of this Policy:	August 1, 2008
Last Revision:	September 1, 2009
Contact for More Information:	UDit Internal Auditor Investment Officer

BACKGROUND

In order to protect credit card information, the credit card industry has introduced security requirements that merchants must follow. These guidelines were established to minimize fraud risk and maximize cardholder protection. Failure of merchants to comply with these guidelines may result in fines or the possibility of not being able to accept credit / debit card payments.

EXECUTIVE SUMMARY AND PURPOSE

To protect against the exposure and possible theft of account and personal cardholder information that has been provided to the University of Dayton during the course of business with the University; and to comply with credit card company requirements for transferring credit card information.

SCOPE

This policy applies to all University of Dayton departments, faculty, staff, students, organizations and individuals who, on behalf of the University of Dayton, handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all University of Dayton locations.

This policy also applies to all external organizations contracted by University of Dayton departments, faculty, staff, students, organizations and individuals to provide outsourced services for credit or debit card processing for University of Dayton business.

DEFINITIONS

Application Server: The computer hosting the application with which the general end-users or point-of-sale (POS) terminals connect.

Credit Card Information: Any cardholder or card information accessed to initiate a credit or debit card transaction.

Cardholder Information Security Program (CISP): A standard of due care for securing Visa cardholder data wherever it is located. Compliance is required of all entities storing, processing, or transmitting Visa cardholder data.

Credit Card Number: Any part or all of the unique number identifying the credit or debit card account for a financial transaction.

Credit Card Processing: Act of storing, processing or transmitting credit or debit cardholder data.

Credit Card Processor: A third party vendor who processes credit and debit card transactions, routes payments to the University of Dayton accounts, charges discounts and adjustment fees and generates statements.

Database Servers: The computer storing the sales and / or credit and debit card numbers.

e-Commerce Application: Any internet-enabled financial transaction application, whether a buying or selling application.

Encryption: Scrambling data in a recoverable format.

ISO 17799: The International Standards Organization document defining computer security standards. ISO 17799 was renumbered ISO 27002 in 2007 to bring it into the ISO 27000 family of standards. This policy document will be changed to reflect this at a later date.

Merchant Number: The unique number identifying the unit accepting credit or debit cards for transactions. This number is necessary to settle the credit and debit card transactions at the appropriate University of Dayton financial institutions. It is also used to identify the specific merchant (departments, faculty, staff, students, organizations and individuals) on the cardholder's monthly credit or debit card statement.

Online Credit Card Acceptance: Credit and debit card payments submitted via the web using a third party vendor's software and passed onto the credit card processor for real-time authorization. The third party vendor securely accepts and stores cardholder and sensitive cardholder data in compliance with the credit card company's security requirements.

Payment Card Industry (PCI): An industry consortium of the founding electronic payment brands – American Express, Discover, JCB, MasterCard, Visa – with the intent "to help facilitate the broad adoption of consistent data security measures on a global basis." The PCI Data Security Standard (PCI DSS) provides a single, comprehensive security standard - security management, policies, procedures, network architecture, software design and other critical protective measures - to help organizations proactively protect customer data.

POS System: Computer or credit card terminals either running as stand alone systems or connecting to a server either at the University of Dayton or at a remote off-site location.

Sensitive Cardholder Data: Any personally identifiable data associated with a cardholder, including but not limited to account number, expiration date, name, address, or social security number, CVC2 / CVV2 validation code (a three digit number imprinted on the signature panel of the card), and data stored on track 1 and track 2 of the magnetic stripe of the card.

Swipe Terminal: POS credit or debit card terminals

POLICY DETAILS

All transactions (including electronic based) that involve the transfer of credit card information must be performed on the systems approved by the University's Investment Officer, after a prior compliance and security review by UDit. All application servers that have been approved for this activity must be housed within UDit and administered in accordance with the requirements of all University of Dayton policies as well as the CISP and PCI DSS. The Investment Officer will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through swipe terminals, while on-line credit card acceptance will be monitored by UDit's IT Risk Management Officer.

Departments needing to accept credit / debit cards and obtain a physical terminal to either swipe or key transactions through the swipe terminals must contact the Investment Officer to obtain a Merchant Number, receive training and be given direction as to how to journalize those transactions on the books of the University.

Departments needing to engage in electronic commerce are required to work with UDit's IT Risk Management Officer to ensure the e-commerce application meets all University policies, ISO 17799 standards and the Payment Card Industry (PCI) Data Security Standard.

Credit Card Security Standard Procedures: It is the policy of the University of Dayton that all departments, faculty, staff, students, organizations and individuals that accept credit and debit cards in the normal pursuit of business do so in a secure manner as set forth by the Payment Card Industry (PCI) Data Security Standard. It is the responsibility of the departments, faculty, staff, students, organizations and individuals to ensure all sensitive cardholder data are protected against fraud, unauthorized use or other compromise. Security standards in place include but are not limited to:

- Ensure your credit / debit card processing terminal is truncating the credit card account number so that only the last 4 digits of the account number are visible. If it is not

truncating, you must contact the Investment Office to have the terminal reprogrammed or replaced.

- Only designated persons should handle sensitive cardholder data.

- All documentation that contains sensitive cardholder data must be kept at all times in a secure area such as a locked file cabinet, desk drawer or office. Keys may be distributed only to a restricted number of designated individuals. Dual control is recommended for access to secured areas. Any locks must be rekeyed or replaced if suspected of compromise or in the event of a termination or transfer of a designated individual.

- Do not store credit card information on desktop computers or on portable electronic media devices. Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

- If credit card information is received via fax machine, the machine must be located in a secure area.

- If credit card information is received via telephone or mail order, do not write information on anything other than an approved form to be used for such purpose.

- In all cases, once the credit / debit card has been processed, use a black magic marker pen or other implement to permanently mask all but the last four digits of the credit card number on the document. Leave the last four digits exposed for future reference.

- Never store the **sensitive authentication data** – full magnetic stripe data, CAV2/CVC2/CVV2/CD or Pin/PIN block.

- No sooner than six months following completion of the credit or debit card transaction, destroy all data associated with the transaction.

Responsibilities of UDit

- Operate and maintain a central secure solution, under the direction of UD Finance & Administrative Services, for the purpose of transacting electronic payments and for data storage, as required for compliance with credit card company regulations and in compliance with the e-Commerce Server Compliance Requirements.

- Provide advice / tools to enable departments clearly to follow industry best practices, access, firewalls, logging, patches, data storage, passwords, encryption and security. Guidance on acceptable technologies and standards may be found on UD's IT Policy web page, http://community.udayton.edu/it/policies/index.php.

- In accordance with UD's IT Incident Handling policy, investigate suspected security breaches and coordinate the response with the appropriate credit card agency, affected customers, and law enforcement as needed.

- Update all PCI related documentation in coordination with any changes within a PCI environment.

- UDit Telecommunications and Networking are the only departments authorized, and only under the direction of the Investment Officer, to logically manage and make approved changes to the network infrastructure supporting UD's PCI environments.

- The IT Risk Managment Office will coordinate the development and distribution of security specific policy and procedures defining responsibilities for all employees and contractors.

- The IT Risk Management Office will monitor and analyze security alerts originating within and without UD and distributing pertinent information to relevant system owners and managers.

Responsibilities of Internal Auditor

- Perform periodic review of all approved units to determine compliance with this policy and other University policies, state / federal laws and regulations, credit card agency regulations, and contracts with financial institutions. These reviews will be both announced and unannounced.

Responsibilities of Investment Office

- Approve each unit requesting to accept credit cards.

- Obtain merchant numbers for each approved unit.

- Obtain approved credit card swipe terminals for each approved unit not using e-commerce for credit and debit card transactions.

- Oversee credit card accounting for each approved unit.

- The Investment Officer will chair the change management process, ultimately responsible for monitoring and controlling all access to data.

- Manage service provider compliance. The Investment Officer will, upon engagement of a service provider, investigate the service provider's PCI fitness and ensure any contract includes acknowledgement of service provider responsibility for any cardholder data they might posses. The Investment Officer will, annually, review service providers' PCI DSS compliance.

Responsibilities of all University Departments, Faculty, Staff, Students, Organizations and Individuals

- Use only application servers, credit card processors, database servers, e-Commerce applications, POS systems, swipe terminals provided by or approved by UDit's IT Risk Management Officer and the Investment Officer.

- Include in all PCI-related agreements that service providers will contractually adhere to the PCI DSS requirements and are responsible for the security of the cardholder date they possess.

- Service agreements must include an acknowledgement that the service provider is responsible for the security of cardholder data held in the provider's possession. UD will actively monitor service providers' PCI DSS compliance status.

- On a regular basis (as defined by individual unit structure), provide appropriate training to all employees associated with credit / debit card processing. UDit's IT Risk Management Officer, Investment Officer, and Internal Auditor will be available to assist in developing the unit specific appropriate training if necessary.

- Processes and procedures must be in place to ensure management approval prior to moving any and all media from a secured area.

- Process (batch) transactions on, at a minimum, a daily basis.

- Record transactions according to the process agreed upon by the Investment Officer and the departments, faculty, staff, students, organizations and individuals.

- Reconcile and verify credit card transactions along with normal accounting reconciliation process.

- Monitor the use of credit card transactions for compliance with this policy and other University policies, state / federal laws and regulations, credit card agency regulations, and contracts with financial institutions.

- Records are subject to audit by both internal and external auditors.

- Notify UDit's IT Risk Management Officer of any suspected security breaches.

- Notify UDit's IT Risk Management Officer and the Investment Officer **IN ADVANCE** of any changes within a PCI environment. Change management procedure and forms may be found on UD's IT Policy web page, http://community.udayton.edu/it/policies/index.php

- At the beginning of the new calendar year, all departments with established merchant accounts or using credit cards in the normal course of their business are required to renew and update their application for merchant account status. Documentation will include a

list of individuals approved to administer user accounts. This signed application should be returned to the Investment Officer. Failure to do so will result in a loss of credit card merchant user privileges.

EXTERNAL CONSEQUENCES

Failure to meet the requirements outlined in this policy will result in suspension of credit card payment capability for the affected units. Additional, fines may be imposed by the affected credit card company, beginning at $10,000 for the first violation up to $80,000 for the fourth violation.

INTERNAL CONSEQUENCES

Failure to meet the requirements outlined in this policy will result in suspension of credit card payment capability for the affected units. Term of suspension will be commensurate with the level of violation of this Policy.

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

Appendix I e-Commerce Server Compliance Requirements

As described on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/index.shtml, the PCI DSS was developed by an industry consortium of the founding electronic payment brands to provide a comprehensive security standard - security management, policies, procedures, network architecture, software design and other critical protective measures - to help organizations proactively protect customer data. While the Council reserves the right to add and revise the requirements to address emerging risks, current requirements fall into the 12 categories below. Please note that these descriptions are not exhaustive and that merchants should refer to the PCI DSS specification available at the website listed above.

1. ***Install and maintain a firewall configuration to protect cardholder data***
   A firewall protects databases with sensitive cardholder data by restricting outside connections, prevents packets from external networks from entering the internal network. The router containing the firewall does not broadcast internal network addresses to the outside network. There is no implied system trust between DMZ and e-commerce systems. Documentation detailing individual merchant environments and maintained by the Investment Officer should provide business justification for services, protocols and ports and record associated firewall and router rule sets. Changes to the environment must be addressed through the change management procedure and forms found on UD's IT Policy web page, http://community.udayton.edu/it/policies/index.php. Router and firewall rule sets should be reviewed semi-annually.

2. ***Do not use vendor-supplied defaults for system passwords and other security parameters***
   System components will be configured in accordance with industry-accepted configuration standards employed within UD's Data Center. UDit and owning staff will monitor software vendor's site regularly for security patches and apply them on the monthly schedule required to comply with PCI requirements.

3. ***Protect stored cardholder data***
   Data stored on the system will be encrypted in accordance with UD's Electronic Use of Confidential Data policy. Unless otherwise specified in UD's retention policies, stored cardholder data – either electronic or paper - will be retained no longer than 6 months unless specifically required for business, legal or regulatory purpose and formally documented by the owning merchant. Disposal of equipment will fall under UD's IT Equipment Disposal and Redisposition policy. Storage media should be logically wiped or physically destroyed when no longer needed.

4. ***Encrypt transmission of cardholder data across open, public networks***
   All credit card data transmitted over the campus network shall be encrypted. E-mail will not be used to send sensitive cardholder data.

5. ***Use and regularly update anti-virus software or programs***
   Anti-virus updating and detection will be completed regularly by UDit.

6. ***Develop and maintain secure systems and applications***

General University staff does not access file information. Access is restricted to the purpose of system and software administration. Access to specific data is limited to a need to know basis with the permission of the merchant department responsible for the data, and only when express permission is given for problem solving purposes. The principle of "least privilege" restricts data access based on a user's need to know. Access to firewall administration is limited to authorized staff. Merchant environments and configuration standards will be reviewed upon purchase/implementation and annually in coordination with individual assessments to ensure individual environments adhere to configuration standards and use only approved technologies. Changes to individual environments, to include user management, must be processed through the change management procedure and forms found on UD's IT Policy web page, http://community.udayton.edu/it/policies/index.php. Daily operational procedures will be developed and maintained for individual merchant environments consistent with and enforcing the requirements of this policy.

7. *Restrict access to cardholder data by business need to know*

All users are uniquely identified prior to accessing cardholder information and system resources.

8. *Assign a unique ID to each person with computer access*

Vendor-supplied defaults are not used for system passwords or other security parameters.

9. *Restrict physical access to cardholder data*

The room used to house the systems is secured with a lock to which only approved staff members have access. Vendor access is restricted and no vendor is allowed in the room without adequate supervision. Paper copies that include any sensitive cardholder data from the credit card transactions are stored in a secure location that is locked and are shredded in accordance to the University of Dayton this Credit / Debit Card Acceptance Policy. In no case will sensitive cardholder data be retained longer than the period stipulated in the University of Dayton policy or Federal regulations. Per UD policy, card holder data is considered confidential. Strict control should be maintained over its distribution and removable media holding such data should be clearly labeled as such and inventories conducted annually. Movement must be processed through the change management procedure and forms found on UD's IT Policy web page, http://community.udayton.edu/it/policies/index.php. Storage media should be logically wiped or physically destroyed when no longer needed.

10. *Track and monitor all access to network resources and cardholder data.*

Logs are available to those with a job related need and allow us to track data access by user ID. These audit trails can be used to reconstruct events and establish accountability. All actions and processes are linked to an active user or system. The audit trails include user identification, type of event, date and time, success or failure, origination of the event, and identity or name of the affected data, system component or resource. The audit trails can reconstruct access to all audit journals, invalid physical and logical access attempts, use of identification and authentication mechanisms, initialization of the audit logs, deletion of objects, actions taken to the compromise of cryptographic keys, changes in the custody of keys or devices or media holding keys, and all encryption key management operations. The audit trails can also reconstruct all actions taken by any

individual with access to the system and when new objects are added to a user's address space. Audit history files are retained for at least one year with 3 months' history available immediately and data from video cameras for at least 3 months. System clocks and times should be synchronized by UDit's configuration standards.

11. *Regularly test security systems and processes*

Tests are conducted regularly to ensure that security controls, limitations, network connections, and restrictions are working to stop or identify unauthorized access attempts.

12. *Maintain a policy that addresses information security for employees and contractors.*

UD's IT policy framework, including usage policies, may be found at http://community.udayton.edu/it/policies/index.php. UD's PCI policy and program will be reviewed by stakeholders annually, including review of threats and vulnerabilities, and after significant change to the infrastructure or merchant environment culminating in explicit approval of risk assessment and mitigation recommendations. List of vendors and service providers will be actively maintained and remote access discontinued immediately upon termination of service. UDit will provide guidance on acceptable technologies, products and their configurations. Distribution of sensitive cardholder data is limited to necessary information only, and only to authorized merchant departments and personnel. Any other distribution must be approved by the Vice President for Finance and Administration and the Associate Provost and CIO. Storage of cardholder data onto local hard drives and removable media is strictly prohibited. Remote access through Cisco's VPN solution will disconnect after 15 minutes of inactivity. Formal security awareness training will be provided upon hire and annually, with employees asked annually to review UD's security and usage policies.

Appendix II Cardholder Information Security Program

Excerpted from the **Visa Cardholder Information Security Program,** available at http://usa.visa.com/business/merchants/cisp_index.html.

CISP Overview

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That's why Visa USA has instituted the **Cardholder Information Security Program (CISP)**. Mandated since June 2001, CISP is intended to protect Visa cardholder data–wherever it resides–ensuring that members, merchants, and service providers maintain the highest information security standard.

In 2004, the CISP requirements were incorporated into an industry standard known as Payment Card Industry (PCI) Data Security Standard resulting from a cooperative effort between Visa and MasterCard to create common industry security requirements. Visa USA maintains CISP as the managing program for data security compliance endorsing the PCI Data Security Standard.

Effective September 7, 2006, the PCI Security Standards Council ("PCI SSC") owns, maintains and distributes the PCI Data Security Standard (DSS) and all its supporting documents. Visa USA, however, continues to manage all CISP compliance enforcement and validation initiatives. In addition, the former QDSC Program has also transitioned to the PCI SSC. Please refer to the Assessors page for more information.

CISP Compliance

CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data and applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. Compliance with CISP means compliance with the PCI Data Security Standard with the required program validation.

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all card brands. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs. Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise. The PCI Data Security Standard consists of twelve basic requirements categorized as follows:

PCI Data Security Standard	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive

	information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

By complying with the PCI Data Security Standard, Visa members, merchants, and service providers not only meet their obligations to the payment system, but also build a culture of security that benefits everyone.

Compliance validation

Separate and distinct from the mandate to comply with the PCI Data Security Standard is the validation of compliance whereby entities verify and demonstrate their compliance status. It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined levels of compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the payment system by merchants and service providers.

For a detailed description of:	**Go to:**
Visa merchant levels of compliance criteria and validation actions	Merchants
Service provider compliance criteria and validation actions	Service Providers

Visa regulations

The Visa USA, Interlink, Inc., and Plus Systems, Inc. Operating Regulations govern the activities of member financial institutions and, by extension, merchants and service providers as participants in the Visa payment system.

Members must comply with CISP and are responsible for ensuring the compliance of their merchants, service providers, and their merchants' service providers. Acquirers must include a CISP compliance provision in all contracts with merchants and agents. Specific compliance requirements and validation criteria are provided at this website.

Appendix III UDit Internal PCI Audit Requirements

At the time of review, the University of Dayton is considered a Level 3 merchant. Technical compliance requirements for that classification are determined by the merchant's acquirer, but should include annual completion of Payment Card Industry (PCI) self-assessment questionnaires well as regular network scans and penetration tests. This document was drafted to detail UDit's responsibilities with regards to ensuring required activities are completed.

Quarterly, UDit will conduct a network scan of PCI environments.

Annually,

1) UDit will contract with an approved scanning vendor to conduct the required quarterly external vulnerability scans

2) UDit will work with the owning unit to address the self-assessment questionnaire:

    a. Collect latest documentation to include statement of compliance from vendor(s)

    b. Prepare/review comprehensive network diagram

    c. Work with the Unit to determine validation type and appropriate self assessment questionnaire

    d. Walk through PCI Data Security Standards (DSS), self assessment questionnaire and vendor statement of compliance with the unit

    e. Coordinate correction/waiver of deficiencies

    f. UDIT/Investment Officer/Unit sign off

UDit will work with owning staff to mitigate any vulnerabilities found and maintain a copy of assessments, findings, notes and resolutions. Documentation will be maintained in the office of the Investment Officer.

This document needs to be reviewed by stakeholders identified in the associated policy annually to address changes to UD's merchant status and PCI requirements.