UNIVERSITY of DAYTON

PCI General Policy

Effective Date: August 2008

Approval: December 17, 2015

Maintenance of Policy: Office of Student Accounts

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.

REFERENCE DOCUMENTS:

1. UDit Incident Handling Policy

APPLICABLE REGULATIONS:

1. Payment Card Industry Data Security Standards (PCI DSS)

POLICY HISTORY:

Approved as Amended

December 17, 2016

Approved in Original Form

August 2008

DEFINITIONS (continued):

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 27000: The International Standards Organization series defining computer security standards.

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:

All transactions (including electronic based) that involve the transfer of credit card information must be performed on the systems approved by the University's Office of the Treasurer after a prior compliance and security review by UDit. All application servers that have been approved for this activity must be administered in accordance with the requirements of all University of Dayton policies as well as the CISP and PCI DSS. The Office of the Treasurer 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 Office of the Treasurer 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 27000 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 Office of the Treasurer 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.

POLICY (continued):

- 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, https://www.udayton.edu/udit/service_level_resources/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 Office of the Treasurer, to logically manage and make approved changes to the network infrastructure supporting UD's PCI environments.

- The IT Risk Management 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 Office of the Treasurer

- Approve each unit requesting to accept credit cards.

POLICY (continued):

- Obtain merchant numbers for each approved unit.

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

- Oversee credit card accounting for each approved unit.

- A representative of the Office of the Treasurer will chair the change management process, being ultimately responsible for monitoring and controlling all access to data.

- Manage service provider compliance. The Office of the Treasurer 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 possess. The Office of the Treasurer 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 Office of the Treasurer.

- 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, Office of the Treasurer, 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 Office of the Treasurer and the departments, faculty, staff, students, organizations and individuals.

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

POLICY (continued):

- 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 Office of the Treasurer **IN ADVANCE** of any changes within a PCI environment. Change management procedure and forms may be found on UD's IT Policy web page, https://www.udayton.edu/udit/service_level_resources/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 Office of the Treasurer. 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. Additionally, 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.