Electronic Use of Confidential Data

Effective Date: February 2008

Approval: December 17, 2015

Maintenance of Policy: UDit & VP for Finance and Administration

PURPOSE: This document details the University of Dayton's policy on the secure electronic access, use, storage, and disposal of confidential information as categorized in Appendix A.

SCOPE: This policy applies to all University personal computing and communication devices and all UD servers and services (whether located at UD or hosted externally) hosting data. Confidential data should not be hosted on personally owned devices.

Individual data elements are classified as *personally identifying* or *business sensitive* in Appendix A. Separate documents within the associated framework will provide detailed standards describing how systems hosting these classifications, as well as public information, must be administered from data collection to system disposal.

A future addendum to this policy should include guidance on the use, storage, and disposal of paper-based confidential information.

POLICY:

The University of Dayton has an obligation to protect the confidential data it collects and processes in pursuit of its business operations. Staff and students will be educated regularly as to the legal and ethical concerns/requirements surrounding confidential data, their own as well as that of fellow students and colleagues, and its handling.

Long used as unique identifiers, the Social Security Number (SSN) is a frequent target for identify theft and other illegal and harmful activities and requires special mention. The University's official position on the use of SSNs, based on executive directive, is to use SSNs only where explicitly required by law or explicitly approved by the Provost.

In all other cases, the University requires the use of a unique University ID (UDID) number. The UDID numbers replace SSNs for identification and as indices to personnel records.

REFERENCE DOCUMENTS:

1. ISO 27002 2013 Sec. #8.2
2. UDit Incident Handling Policy

APPLICABLE REGULATIONS:

Including, but not limited to:

1. Family Educational Rights and Privacy Act (FERPA)
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
3. Payment Card Industry Data Security Standards (PCI DSS)

POLICY HISTORY:

Approved as Amended

December 17, 2015

Approved in Original Form

February 2008

POLICY (continued):

The following guidelines govern information classified as either *personally identifying* or *business sensitive*:

- Disclosure: Forms and web pages requesting confidential data should contain a privacy disclosure outlining, but not limited to, what will be collected, who authorized collection of this data, how the data will be used, how long the data will be maintained, how to correct data elements and who will have access to data
- Storage: Servers, whether located at UD or hosted externally, containing confidential data must be implemented in accordance with documented standards and subject to audit. All devices (including servers, backup tapes, desktop/laptop computers, removable media and mobile communication devices) hosting confidential data require encryption of data at rest or suitable compensating control

- Access: Access to confidential data is restricted to those with a demonstrated business need and requires regular renewal of a confidentiality agreement
- Transmission: Transmission of confidential data requires use of encrypted transport protocols

- Discovery: Automated tools will be provided and used to discover and log existence of confidential data on servers and personal computing/communications devices
- Disposal: Media housing confidential/sensitive data must be physically destroyed or sanitized in accordance with NIST standards or equivalent upon disposal or redeployment in accordance with UD's Equipment and Removable Media Disposal policy

Servers will be periodically audited in accordance with UD's Server Audits policy to ensure adherence to standards for access, use, and storage of data types as outlined by this policy and related standards documents. An inventory of Approved Hosts of Confidential Information will be maintained, reviewed, and approved regularly by the VP for Finance and Administrative Services (or a delegate). Any exceptions to the framework requirements must be approved and documented.

The authority to monitor and ensure compliance will be the responsibility of the UDit Risk Management Officer in cooperation with the CIO and VP for Finance and Administrative Services. Violations of this policy will be considered serious and will result in disciplinary action. An employee who violates this policy may be held responsible for the cost of mitigation due to loss or breach.

Appendix A
Data Classification

This appendix attempts to identify the individual elements of data categorized as either *personally identifying* or *business sensitive*.

I. Directory Information

The specific data elements that the University considers directory information is maintained in the definitions section of UD's Policy on Disclosure of Student Records ("FERPA" Policy) at http://www.udayton.edu/policies/enrollment/ferpa/ferpa_policy_page.php. The University is allowed, but not obligated, to divulge this information without student consent unless the student specifically opts out.

II. Personally Identifying Information

The following data elements fall into the category of personally identifying and are further categorized by applicable regulation:

HIPAA: Protected Health Information (http://www.hhs.gov/ocr/hipaa/)

Federal law protects the health records and privacy of individuals. The Privacy Rule establishes minimum standards for protecting the privacy of individually identifiable health information. Individually identifiable health information, somewhat confusingly, includes elements such as name that would normally be considered directory information. The following 18 elements (http://privacyruleandresearch.nih.gov/pr_08.asp#8a) could be used to identify the individual or the individual's relatives, employers, or household members.

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct and ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
    - o The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people
    - o The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Facsimile numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers

- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs)
- Internet protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voiceprints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

Exceptions to the HIPAA regulations by "educational agencies" are defined at http://www4.law.cornell.edu/uscode/20/1232g.html.

FERPA: Student Records (http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html)

Federal law protects the privacy of student education records. Schools must list what they consider to be directory information. UD assumes all elements of the student record, except for those items listed at the beginning of this appendix, to be confidential. Examples of confidential information include:

- Grades/Transcripts
- Class lists or enrollment information
- Student Financial Services information
- Athletics or department recruiting information
- Credit Card Numbers
- Bank Account Numbers
- Wire Transfer information
- Payment History
- Financial Aid/Grant information/Loans
- Student Tuition Bills

Credit and Debit Cards (https://www.pcisecuritystandards.org/)

Security standards compiled by members of the Payment Card Industry (PCI) Security Council.

- Cardholder Data
  - o Credit Card Number
  - o Cardholder Name *
  - o Service Code*
  - o Expiration Date*
- Sensitive Authentication Data
  - o Full Magnetic Stripe**
  - o CVC2/CVV2/CID**
  - o PIN/PIN Block**

* Elements must be protected if stored in conjunction with the credit card number
** Storage is not permitted

III. Business Sensitive

The categories of data listed below, while not necessarily regulated, are considered valuable to the University of Dayton. Loss of this information might lead to embarrassment, risk to safety, competition, etc.

- Donor Information
- Employee information
- Financial Information
- Infrastructure Information
- Management Information
- Research Information

This document is not comprehensive and should be revisited regularly to clearly identify sensitive data elements to all members of the University community. In the case of a breach of any of the elements listed in this appendix, incident response and handling procedures should be initiated through UDit and the IT Risk Management Officer. Questions can be addressed to the responsible office listed in this policy.