DEPAUL UNIVERSITY

Information Security Policy

Category: Operations
Responsible Department: Information Services
Responsible Officer: Vice President for Information Services
Effective Date: 3/31/2017

Policy Summary

DePaul has adopted this Information Security Policy in order to:

- Ensure the security, availability, privacy, and integrity of DePaul's information systems, networks and data;
- Outline procedures for reporting breaches of information security; and

Ensure compliance with various federal and state laws as well as other DePaul information security-related policies and procedures.

Scope

This policy affects the following groups of the University:

- Entire University Community

This policy affects all members of the University Community.

Policy

A. DEFINITIONS

'Covered Data' includes, but is not limited, to those data items listed below:

- Social security numbers
- Credit card numbers
- Debit card numbers
- Bank account numbers
- Passwords, pins, certificates and similar data that permit access to financial accounts
- Driver's license numbers
- State (and other government) identification card numbers/information
- Passport and citizenship information (including passports of other countries)
- Income and credit information
- Tax returns

- Statements of assets and/or liabilities
- Financial aid application materials
- Loan information (including repayment status)
- Scholarship application materials
- Donor/potential donor information
- Payroll information
- Other personally identifiable financial information not otherwise publicly available
- Legal files
- Health-related information (including DePaul Community Mental Health Center data, student-athlete injury and rehabilitation data, and any other person's health care or health care payment information)
- Sensitive student information (including student grades, information on athletic compliance forms, official and unofficial transcripts, and any other student record information required to be protected by FERPA)
- Personnel files
- Other personal human resource information
- Aggregations of names and/or contact information of DePaul applicants, students, faculty and/or staff
- Sensitive competitive data
- Research data and advising/counseling data containing sensitive information
- Public safety incident reports
- Lists of hazardous materials stored at DePaul
- Insurance policy numbers

'Privacy Team' means representatives from appropriate university units taking steps to (i) connect the Responsible Officer and the appropriate university units, (ii) ensure effective working relationships between the Responsible Officer and the DePaul community and (iii) otherwise help formulate and execute this Information Security Policy.

'Service Providers Having Covered Data Access' means third parties who are provided access to Covered Data including, without limitation, any business retained to process, analyze, transport, backup or dispose of Covered Data, collection agencies and consultants that work on a DePaul system or device.

'University IS Policies' means this Information Security Policy and other official DePaul Policies and Procedures that relate to information security including, without limitation, the following policies (a brief summary of each policy is also provided):

- Access to and Responsible Uses of Data. Explains the approval process and requirements for system data (i) access (e.g., appropriate management level approval, request for data access forms); (ii) use (e.g., need-to-know type requirements); and (iii) security (e.g., user IDs/passwords; users required to protect against unauthorized access).
- Health Information Privacy. Protects personal health information created, received or maintained by DePaul and designates a Chief Privacy Compliance Official (CPCO) who is responsible for ensuring DePaul fulfills its legal obligations under HIPAA. The

CPCO specifically requires departments to establish their own procedures which, in turn, are centrally housed with the CPCO.

- Acceptable Use Policy/Network Security. Describes acceptable and unacceptable uses of DePaul's computer resources (e.g., prohibits transmitting unsolicited emails, attempting to gain unauthorized access to DePaul's computer resources, intercepting communications, collecting personal data).
- Disposal of Equipment & Assets. Requires departments to follow established procedures for discarding DePaul equipment (which may contain Covered Data).
- Access to and Responsible Use of Student Email Address Information. Amplifies that there are restrictions on sending mass e-mails to students.
- DePaul University Computing Policy. Provides general principles, guidelines and security requirements for all computing environments at DePaul University.

B. COMMUNITY MEMBER RESPONSIBILITIES

Each member of the DePaul community must:

1. Comply with all University IS Policies.
2. Report all breaches to (or losses/improper uses of) DePaul data, systems or devices. Such events must be immediately reported to DePaul's Director of Information Security using the e-mail security@depaul.edu. To report potential abuses, use the e-mail abuse@depaul.edu. If health-related information is involved, DePaul's Health Information Privacy policy must also be followed.
3. Ensure oversight of Service Providers Having Covered Data Access. Any Service Provider Having Covered Data Access must (a) have a signed contract in place with DePaul and (b) maintain appropriate safeguards to protect DePaul's data. DePaul employees engaging any such service provider must make certain that:
    - The Office of the General Counsel has reviewed the contract with the service provider, regardless of the contract's dollar amount; and
    - The Director of Information Security has reviewed the anticipated use(s) of the data to determine whether the service provider is reasonably capable of maintaining appropriate safeguards to protect any Covered Data the service provider may have access to.

DePaul community members who fail to comply with this Information Security Policy are subject to disciplinary action including, without limitation, reprimand, loss of network access privileges, suspension or discharge/expulsion.

C. RESPONSIBLE OFFICER RESPONSIBILITIES

The Responsible Officer in his role as Chief Information Privacy Official shall oversee the on-going implementation and execution of the following five (5) responsibilities:

1. Assessing the risks associated with DePaul data, systems or devices. Risk assessment models and methodology applicable to information security will be developed and implemented in the applicable DePaul departments. Such risks assessments will: (a) help identify '*reasonably foreseeable*' internal and external risks to the security and privacy of DePaul data that may result in unauthorized disclosure,

misuse, alteration, destruction or other compromise of such data; (b) assess the sufficiency of any safeguards already in place to control these risks; and, (c) include reviews of the following broad areas:

- Employee selection, training and management. Such reviews will include evaluating the effectiveness of the existing safeguards relating to access to and use of Covered Data.
- Information systems. Such reviews will include evaluating the effectiveness of the existing safeguards relating to network and software design, as well as the processing, storage, transmission and disposal of Covered Data and the procedures for monitoring potential system threats and updating such systems (e.g., by implementing patches or other software fixes).
- The detection, prevention and response to attacks and other system failures. Such reviews will include evaluating the effectiveness of existing safeguards relating to methods of detecting, preventing and responding to attacks and other system failures as well as procedures for coordinating responses to network attacks and having incident response teams and policies.

2. Designing, implementing and monitoring safeguards to help minimize the risks associated with DePaul data. Safeguards to control the risks identified through the risks assessments described above will be designed and implemented. The effectiveness of such safeguards will be regularly tested and monitored.

3. Determining whether there has been a 'Breach Requiring Notice' and, if so, notifying the applicable people. When circumstances arise suggesting that there may have been a Breach Requiring Notice (defined below), the Responsible Officer shall work with additional members of Information Services and others in order to (a) evaluate all of the pertinent facts and (b) determine whether or not there has been a bona fide Breach Requiring Notice.

Following the discovery or notification of a bona fide Breach Requiring Notice, the Responsible Officer shall cause the applicable people (including those entitled to notice by law) to be notified of the breach via any one of the following methods:

- E-mail notice;
- Written notice;
- Substitute notice (if the Responsible Officer reasonably determines that (i) DePaul does not have sufficient contact information to provide e-mail or written notice to the affected persons or (ii) the aggregate cost of providing such notice would greatly outweigh the aggregate benefit expected to be gained by the affected persons if such persons received such notice, substitute notice may be provided by placing a conspicuous posting on DePaul's website); or
- Any reasonable combination of e-mail, written or substitute notice. (if the Responsible Officer reasonably determines, after considering all then available pertinent facts, that such a combination is the most sensible approach).

The above evaluations, determinations and notices shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the

scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system(s).

'Breach Requiring Notice' means an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Notice Data (defined below) but does NOT include the good faith acquisition of Notice Data by an employee or agent of DePaul for a legitimate purpose, provided that such Notice Data is not (i) used for a purpose unrelated to DePaul's business or (ii) subject to further unauthorized disclosures.

'Notice Data' means a combination of at least one of the names in List I below and at least one of the data elements in List II below (where EITHER the name or data element is not adequately encrypted or redacted):

I. One or more of these names
- First name and last name; or
- First initial and last name.

IN COMBINATION WITH

II. One or more of these data elements
- Social Security number;
- Driver's License number;
- State Identification card number; or
- Account number or credit or debit card number.

4. Staying current on the laws relating to information security. Given the rapid changes in the laws relating to this Information Security Policy's subject matters, the Responsible Officer shall consult regularly with the Office of the General Counsel to stay current on such laws. Such consultations may consider, among other things, understanding more precise definitions for a Breach Requiring Notice, Notice Data and similar terms as such terms are further interpreted by applicable laws, regulations and rulings.

5. Evaluating and adjusting all information security-related policies. This Information Security Policy, other University IS Policies and IS Guidelines (defined below) will be continually evaluated and adjusted , in light of:

- The results of testing and monitoring;
- Any pertinent changes in the laws;
- Any material change to DePaul's operations or business arrangements; or
- Any other circumstances that (DePaul knows or has reason to know) may have a material impact on this Information Security Policy.

The Responsible Officer is responsible for ensuring DePaul's ultimate compliance with this Information Security Policy. Where applicable, however, the Responsible Officer shall receive appropriate support from: (i) the Privacy Team, (ii) other members of the Office of the General Counsel, the Office of Institutional Compliance, the Office of the Secretary, Information Services, Internal Audit, and (iii) other members of the DePaul community having the pertinent authority and

responsibility. The Responsible Officer may also consider and leverage other University IS Policies and IS Guidelines when carrying out the Responsible Officer's responsibilities. IS Guidelines are technical and other security guidelines maintained by Information Services which:

- Strive to reflect the best information security practices for DePaul's industry;
- Consider the objectives contained in industry standard guidelines; and
- Include the guidelines of the Information Security Team of DePaul University which, among other things, relate to appropriate uses DePaul's technical resources (e.g. , computers, networks and applications) and other technology security issue s (e.g. , access, passwords, handling of information, technical security practices)

Procedures

Procedures (to report breaches to, or improper uses, of DePaul data, systems or devices)

If a member of the DePaul community becomes aware of any breach to (or loss/improper use of) DePaul data, systems or devices, he/she must immediately report such event(s) to DePaul's Director of Information Security using the e-mail security@depaul.edu.

To report potential abuses, use the e-mail abuse@depaul.edu.

If health-related information is involved, DePaul's Health Information Privacy policy must also be followed.

Divisional Collaborations

In addition to the Privacy Team, the following DePaul departments are some of the DePaul divisions that are expected to continually collaborate on the subject matters covered by this Information Security Policy:

- The Office of Institutional Compliance;
- The Office of the General Counsel;
- The Office of the Secretary;
- Internal Audit; and

Other areas at DePaul with access to Covered Data.

Contact Information

Director of Information Security
Website: http://security.depaul.edu
Email: security@depaul.edu

Appendices

APPENDIX A: Access to and Responsible Uses of Data (Policy)
APPENDIX B: Health Information Privacy (Policy)

APPENDIX C: Acceptable Use Policy/Network Security
APPENDIX D: Disposal of Equipment & Assets (Policy)
APPENDIX E: Access to and Responsible Use of Student Email Address Information (Policy)
APPENDIX F: DePaul University Computing Policy

History/Revisions

Origination Date: 12/07/2005
Last Amended Date: 03/31/2017
Next Review Date: N/A