Student Financial Aid Information Security & Privacy (GLBA Compliance)

Category: Operations
Responsible Department: Office of Financial Aid
Responsible Officer: Vice President for Enrollment Management
Effective Date: 04/08/2024

Policy Summary

This policy summarizes the university's program and procedures for protecting student financial aid information obtained by DePaul in support of the administration of Federal student financial aid programs, as required by the Gramm Leach Bliley Act (the "GLBA") the Federal Trade Commission's Standards for Safeguarding Customer Information (the "Safeguards Rule"), the Higher Education Act (the "HEA"), and the Privacy Act of 1974, as amended (the "Privacy Act").

Scope

This policy affects the following groups of the University:

- Entire University Community

Policy

A. The Program

As required by the GLBA and the Safeguards Rule, DePaul maintains a comprehensive, written information security program designed to protect student financial aid information obtained by DePaul in support of the administration of Federal student financial aid programs (the "Program"). The Program is specifically designed to (i) ensure the security and confidentiality of student financial records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to students.

This policy, along with other applicable university policies and procedures related to data privacy and security, constitutes the Program. Such other policies include, but are not limited to:

- Access to and Responsible Use of Data
- Contract Requirements and Procedures
- DePaul University Privacy Statement
- FERPA Compliance
- Information Security
- Payment Card Acceptance

B. Scope of the Program

The Program applies to any record maintained by DePaul, or on behalf of DePaul, that contains Nonpublic Financial Information about a student or other third party who has a relationship with the institution. For purposes of the Program, the term "Nonpublic Financial Information" shall mean any information (i) a student or other third party provides in order to obtain a financial service from DePaul, (ii) about a student or other third party resulting from any transaction with DePaul involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with DePaul providing a financial service to that person.

Data from the Free Application for Federal Student Aid ("FAFSA") or the Institutional Student Information Record ("ISIR") that is provided to DePaul by the US Department of Education is a unique category of Nonpublic Financial Information that falls within the scope of the Program. Pursuant to the HEA, the Privacy Act, and US Department of Education guidance, use of FAFSA, ISIR, or FAFSA Submission Summary data by DePaul will be strictly limited to the application, award, and administration of aid awarded under federal student aid programs, state aid, or aid awarded by eligible institutions.

C. Elements of the Program

1. Designated Qualified Individual

The university's Chief Information Privacy Official is the designated qualified individual responsible for overseeing, implementing, and enforcing the Program.

2. Risk Assessment

The Program is based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Nonpublic Financial Information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. Risk assessment is an ongoing process, which is documented in the Access to and Responsible Use of Data policy.

3. Safeguards

The Program requires DePaul employees to implement various safeguards that are intended to control the risks identified in the Access to and Responsible Use of Data policy. These safeguards are documented in the Security Classification and Controls Matrix, which is an appendix to the aforementioned policy. They include, but are not limited to:

a. Technical and physical access controls that (i) authenticate and permit access only to authorized users to protect against the unauthorized acquisition of Nonpublic Financial Information; and (ii) limit authorized users' access only to Nonpublic Financial Information that they need in order to perform their duties and functions, or, in the case of students, to access their own information.

b. Annual assessments conducted by Information Services and Information Security, identifying the data, personnel, devices, systems, and facilities that enable DePaul to achieve its business purposes, in accordance with their relative importance to the university's business objectives and risk strategy.

c. Encryption of all Nonpublic Financial Information transmitted by the university, as well as additional effective controls that serve to protect Nonpublic Financial Information at rest. For more information, please see the Access to and Responsible Use of Data policy.

d. Vendor Risk Assessments, which are conducted by Information Security prior to the purchase of any externally developed application that will be used to transmit, access, or store DePaul's Nonpublic Financial Information. A Vendor Risk Assessment involves a thorough review of a vendor's data privacy and security standards, followed by an identification of any significant risks to the contracting university business or academic unit. Vendor Risk Assessments are conducted prior to executing a contract for applicable services, and reassessed annually for vendors with access to Highly Sensitive Data, as defined in the Access to and Responsible Use of Data policy. For additional information regarding the Vendor Risk Assessment process, please consult the Information Services Knowledgebase.

e. Multi-factor authentication, which is required for any individual accessing systems that fall within the scope of this policy, including those used to transmit, access, or store Nonpublic Financial Information.

f. A Records Management policy and a Records Retention Schedule, which provide for (i) Nonpublic Financial Information to be retained only for the period such information is necessary for legitimate business purposes, or for the period the university is otherwise required to retain such data pursuant to applicable law, regulation, or industry best practice; and (ii) Nonpublic Financial Information to be disposed of in an approved, secure manner. Like all university policies, the Records Management policy is subject to routine three-year review, and may be updated off-cycle by request.

g. Minimum security standards required of all vendors handling Nonpublic Financial Information, which are assessed and monitored through the Vendor Risk Assessment process.

h. Procedures and controls designed, managed, and maintained by the Office of Information Services to monitor and log the activity of users authorized to access applications that manage Nonpublic Financial Information and detect unauthorized access or use of, or tampering with, customer information by such users.

4. Regular Testing of Safeguards

The safeguards outlined in this policy are routinely tested through assessments conducted by Information Services and Information Security. In addition, Internal Audit completes an annual risk assessment and audit plan.

5. Policy Implementation

Various university policies form the basis of the Program. New or substantial changes to existing policies that the Chief Information Privacy Official deems necessary or advisable in furtherance of the Program may be introduced in accordance with the procedures outlined in the university policy entitled Establishing a University Policy.

6. Management of Information System Service Providers

The Chief Information Privacy Official will coordinate Information Security with Procurement, the Office of General Counsel, Compliance and purchasing business and academic units to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for Nonpublic Financial Information of students and other third parties to which they will have access. This is largely handled through Vendor Security Reviews (see above). However, per the Contract Requirements and Procedures policy, the Office of General Counsel will also work with these departments to incorporate standard contractual protections applicable to third party service providers, which further require such providers to implement and maintain appropriate safeguards.

7. Routine Evaluation and Adjustment of the Program

The Chief Information Privacy Official will routinely evaluate and adjust the Program, as appropriate. Adjustments may be made based on the risk assessments conducted per Section 2, above, the results of the testing of the safeguards outlined in Section 4, above, or any other change in circumstances or industry best practices with the potential to impact DePaul's data security. Every university policy that comprises the Program will be reviewed, at minimum, every three years, as required by the policy entitled Establishing a University Policy.

8. Incident Response Plan

The Program includes a written Incident Response Plan, which outlines the processes university business and academic units will follow in response to a security incident. The Incident Response Plan is retained and managed by the Director of Information Security. DePaul's Information Security team is responsible for enacting the Incident Response Plan and coordinating the communications and response efforts required thereunder.

The Incident Response Plan consists of the following phases:

- Preparation
- Identification
- Notification

- Incident Analysis
- Remediation
- Recovery
- Lessons Learned

The Incident Response Plan contemplates collaboration between the following individuals, university units, and external organizations, depending on the severity of the incident:

- Director of Information Services
- Director of Infrastructure
- Director of Services
- Director of Development
- DePaul Business Function Area / Data Owner
- Dean of Students
- Human Resources
- Office of the General Counsel
- Technology Vendors
- Public Safety
- Internal Audit
- Law Enforcement
- University Marketing Communications
- Other Senior Executives
- DePaul's Internet Service Provider
- US-CERT, REN-ISAC, FIRST (Forum of Incident Response and Security Teams)
- Internet Service Provider of Attacker
- Affected External Parties
- Cyber Security Insurer
- Forensic Consultant
- External Legal Counsel
- Credit Monitoring Services

9. Regular Reporting

The Chief Information Privacy Official meets at least annually with the university's Board of Trustees to report on the Program. These reports include a summary of any known security incidents involving data that falls within the scope of the Program.

Procedures

University-wide procedures related to the Program are specified in the various policies and procedure documents referenced throughout this policy. Additional, non-conflicting, departmental procedures regarding the protection of Nonpublic Financial Information may be developed by the individual university business and academic units that handle such data.

Divisional Collaborations

Information Services
Financial Affairs
Office of the General Counsel
Compliance and Risk Management

Contact Information

Office of Financial Aid
Karen LeVeque-Szawara
Assistant Vice President – Financial Aid
(312) 362-8525
kleveque@depaul.edu

Chief Privacy Compliance Official
Vice President of Information Services
Bob McCormick
(312) 362-8200
bmccormi@depaul.edu

Appendices

None.

History/Revisions

Origination Date: 04/08/2024
Last Amended Date:
Next Review Date: N/A