UNIVERSITY OF NOTRE DAME

Information Security Policy

Responsible Executive: Chief Information Officer
Responsible Office: Office of Information Technologies
Approved by: Information Governance Committee
Issued: July 2009
Revised: September 2018

1. INTRODUCTION

The purpose of this policy is to establish a security framework designed to protect Notre Dame information assets from accidental or intentional unauthorized access, modification, damage, or deletion, while also preserving the open-information sharing requirements of its academic culture. Standards and procedures related to this policy are published separately and updated as required.

2. POLICY STATEMENT

Information that Notre Dame or its agents use in the course of conducting University business is an institutional resource. Although individuals, offices, departments, programs, or schools may have responsibilities for creating and maintaining portions of University information and University records, the University itself retains ownership of, and responsibility for, the information and its protection.

Information security designations and handling requirements will be created and maintained by the Information Governance Committee in partnership with Data Stewards responsible for specific data and data elements. All information assets will be secured according to the standards and procedures established by the Office of Information Technologies (OIT) Information Security and Compliance unit.

2.1. Information Governance Committee

The Executive Vice President will appoint members to the Information Governance Committee (IGC). The Information Governance Committee will be chaired by the Vice President for Information Technologies, and will:

- Appoint data stewards for the University
- Define which data elements are Highly Sensitive
- Serve as the data steward for Highly Sensitive data elements
- Create handling requirements for each Highly Sensitive data element
- Regularly review all standards related to this policy
- Arbitrate disputes related to this policy

Appeals of Information Governance Committee decisions can be made in writing to the Executive Vice President.

2.2. Campus Data Steward

The Campus Data Steward will:

- Maintain a list of Data Stewards and their designees as appointed by the IGC
- Maintain a current list of Highly Sensitive data elements
- Ensure that appropriate handling requirements for information and data access are established by each Data Steward for their area of stewardship
- Ensure that appropriate handling requirements are implemented for University information assets

2.3. Data Stewards

Data Stewards are appointed by the Information Governance Committee and will:

- Assign information under their stewardship to one of three security designations: public, internal, or sensitive, based upon the information's intended use and the expected impact if disclosed
- Bear primary responsibility for decisions regarding handling requirements for the data under their stewardship
- Coordinate activities with areas outside their own when data usage, access and/or handling impacts extend beyond their own unit
- Identify and authorize Designates for acting as the Data Steward's proxy for activities within their stewardship

2.4. Office of Information Technologies Information Security and Compliance

- Create standards and procedures that meet the information asset handling requirements defined by the Data Stewards
- Submit information asset handling standards and procedures to the responsible Data Stewards for approval
- Investigate and report to the IGC suspected violations of security policy

The University's policy is to comply with all applicable legislative, regulatory, and contractual requirements concerning information security. University Information Security handling requirements and standards may exceed legally prescribed requirements.

3. SCOPE

This policy applies to faculty, staff, students, and all others granted use of University information assets and defines their responsibility for the protection and appropriate use of University information, applications, computer systems, and networks.

4. DEFINITIONS

Information assets: All University data including but not limited to verbal, printed, or records represented as audio, video, still picture, or a combination of these.

Information Handling Requirements: Mandated handling of information assets including who may handle it, when they may handle it, in what circumstances and for what purpose.

Standard: Expected user behavior when interacting with University information assets, based on the security designation and information handling requirements.

Procedure: Technical specifications, methodologies and specific instruction for data (format, structuring, tagging, storage, transmission, manipulation, reporting), and use of data.

Security Designation: University data is categorized into one of the following security designations based upon IGC or Data Steward requirements and its intended use and expected impact if disclosed.

Public
Information intended for broad use within the University community at large or for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy and confidentiality.

Internal
Information intended for limited use within the University that, if disclosed,

could have an adverse effect on the operations, assets, or reputation of the University. Information designated as Internal would not generally compromise the University's obligations concerning information privacy and confidentiality.

Sensitive
Information intended for limited use within the University that, if disclosed, could be expected to have a specific and serious adverse effect on the operations, assets, or reputation of the University, or to compromise the University's obligations concerning information privacy and confidentiality.

Highly Sensitive
Information that meets the criteria for sensitive information and which in the judgment of the IGC requires additional oversight and control due to the reputational, financial, or operational impact it may have on the University.

5. RESPONSIBILITIES

Executive Vice President	1. Appoint members of the Information Governance Committee.
Vice President for Information Technology	1. Serves as the chair of the Information Governance Committee.

Information Governance Committee	1. Appoint data stewards for the University. 2. Define which data elements are Highly Sensitive 3. Serve as the data steward for Highly Sensitive data elements 4. Regularly review all requirements related to this policy 5. Arbitrate disputes related to this policy
Campus Data Steward	1. Maintain a list of data stewards and designates 2. Serve as the data steward designate for Highly Sensitive data elements 3. Maintain a current list of Highly Sensitive data elements 4. Ensure that appropriate requirements for information and data access are established by each Data Steward for their appropriate scope of stewardship 5. Ensure that appropriate Data Governance is completed for University information assets.
Data Steward	1. Bear primary responsibility for decisions regarding data usage, access and handling for the data under their stewardship. Stewardship of Highly Sensitive data elements is reserved for the Information Governance Committee 2. Coordinate activities with areas outside their own when data impacts extend beyond their own unit
Information Security and Compliance	1. Create standards and procedures that meet the information asset handling requirements defined by the Data Stewards and based on the NIST Cybersecurity Framework 2. Submit information asset handling standards and procedures to the responsible Data Stewards for approval 3. For information assets that require secure handling but are not under the authority of a Data Steward, create information asset handling requirements, standards and procedures based on the NIST Cybersecurity Framework. 4. Investigate and report to the IGC suspected violations of security policy

Faculty, Staff, Students	1. Protect the privacy and security of University data and information, applications, computer systems, and networks under their control. 2. Adhere to all relevant information handling requirements. 3. Report suspected violations of this policy to the Director of Information Security.

6. POLICY ENFORCEMENT

Information Security and Compliance in Office of Information Technologies will investigate suspected violations. The Office of Information Technologies may recommend disciplinary action in accordance with University codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following:

1. Suspension or termination of access
2. Disciplinary action up to and including termination of employment
3. Student discipline in accordance with applicable University policy
4. Civil or criminal penalties

Report suspected violations of this policy to the Office of Information Technologies Information Security and Compliance, or to the appropriate Data Steward. Reports of violations are considered Sensitive Information until otherwise designated.

7. REFERENCE DOCUMENTS

7.1 Notre Dame Policy or Document	Web Address
Highly Sensitive Information Handling Standard	http://oit.nd.edu/policies-standards/information-technology-standards/highly-sensitive-information-handling-standard/
Information Security Policy	https://policy.nd.edu/assets/185243/information_security_policy_2015.pdf
Information Technology Incident Response Policy	https://policy.nd.edu/assets/185245/information_technology_incident_response_2015.pdf
Intellectual Property Policy	https://policy.nd.edu/assets/203061/intellectualpropertypolicy.pdf
NIST Cybersecurity Framework	https://www.nist.gov/cyberframework/framework

NetID Access to University Information Technology Resources	https://policy.nd.edu/assets/185252/net_id_access_to_university_it_resources_2015.pdf
Records Management and Archives Policy	https://policy.nd.edu/assets/185265/records_management_archives_2015.pdf
Responsible Use of Information Technologies at Notre Dame	https://policy.nd.edu/assets/185268/responsible_use_it_resources_2015.pdf

7.2. External Documents	**Web Address**
National Institute of Standards and Technology Cybersecurity Framework	https://www.nist.gov/cyberframework
Family Educational Rights and Privacy Act (FERPA)	http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Gramm-Leach-Bliley Act (GLBA)	https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
Health Insurance Portability and Accountability Act (HIPAA)	https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html
Indiana Disposal of Personal Information (Indiana Code 24-4-14)	http://www.in.gov/legislative/ic/code/title24/ar4/ch14.html
Payment Card Industry Data Security Standard (PCI DSS)	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

8. CONTACTS

Subject	**Office or Position**	**Office Email or URL**
Data Handling Requirements	Campus Data Steward	datasteward@nd.edu
Standards	Office of Information Security	infosec@nd.edu