UNIVERSITY OF NOTRE DAME

Information Security Policy

POLICY 7.1

Responsible Executive: Chief Information Officer
Responsible Office: Office of Information Technologies
Approved by: Information Governance Committee
Issued: July 2009
Revised: June 2015

1. INTRODUCTION

The purpose of this policy is to protect Notre Dame's information resources from accidental or intentional unauthorized access, modification, or damage, while also preserving the open information sharing requirements of its academic culture.

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.

Information handling standards and classifications will be created and maintained by the Information Governance Committee in partnership with Data Stewards responsible for specific data and data elements in order to properly protect University data.

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
- 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 Designates as appointed by the IGC
- Maintain a current list of Highly Sensitive data elements
- Ensure that appropriate standards for information and data access are established by each Data Steward for their area of stewardship.

- Ensure that appropriate Data Governance is completed for University information

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 classifications: public, internal, or sensitive, based upon the information's intended use and the expected impact if disclosed.
- Bear primary responsibility for decisions regarding data usage and handling for the data under their stewardship. Stewardship of Highly Sensitive data elements is reserved for the Information Governance Committee
- 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 Information Handling Standards

The Information Governance Committee will create handling standards for each Highly Sensitive data element. Data stewards may create standards for other data elements under their stewardship. These information handling standards will specify controls to manage risks to University information and related assets based on their classification. All individuals at the University are responsible for complying with these controls.

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

3. SCOPE

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

4. DEFINITIONS

Security Classifications University data is categorized into one of the following classifications based upon IGC or Data Steward designation 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 classified 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 standards 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 standards 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

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
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 standards. 3. Report suspected violations of this policy to the Director of Information Security.

6. POLICY ENFORCEMENT

The Office of Information Technologies will investigate suspected violations, and 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, or to the appropriate Data Steward. Reports of violations are considered Sensitive Information until otherwise classified.

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	http://policy.nd.edu/policy_files/InformationSecurityPolicy.pdf
Information Technology Incident Response Policy	http://policy.nd.edu/policy_files/InformationTechnologyIncidentResponsePolicy.pdf
Intellectual Property Policy	http://policy.nd.edu/policy_files/IntellectualPropertyPolicy.pdf

NetID Access to University Information Technology Resources	http://policy.nd.edu/policy_files/NetIDAccesstoUniversityITResources.pdf
Records Management and Archives Policy	http://policy.nd.edu/policy_files/RecordsManagementandArchivesPolicy.pdf
Responsible Use of Information Technologies at Notre Dame	http://policy.nd.edu/policy_files/ResponsibleUseITResourcesPolicy.pdf

7.2. External Documents	**Web Address**
Code of practice for information security management; ISO 27002	http://www.iso.org/iso/catalogue_detail?csnumber=50297
Family Educational Rights and Privacy Act (FERPA)	http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Gramm-Leach-Bliley Act (GLBA)	http://banking.senate.gov/conf/
Health Insurance Portability and Accountability Act (HIPAA)	http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf
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)	http://www.ntobjectives.com/datasheets/pcd_manual.pdf

8. CONTACTS

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