



1. INTRODUCTION

The purpose of this policy is to protect Notre Dame's information resources from accidental or intentional unauthorized access or damage, while also preserving the open information sharing requirements of its academic culture. The Officers of the University expect University information in any form—and related assets—to be accurate, available for authorized use, and protected from misuse or modification.

This policy lays the foundation for a common understanding of information security at Notre Dame based upon the generally accepted information security principles of confidentiality, integrity and availability. Confidentiality limits information access to authorized users. Integrity protects information against unauthorized modification. Availability ensures that information is accessible when needed. Together, these three principles ensure that University information can be used in support of the pursuit of the University's goals of teaching, research, and service.

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. University Officers will appoint [Data Stewards](#) and charge each with responsibility for a segment of University information and with participating as members of the [Data Oversight Committee](#). [Data Stewards](#) will assign information under their stewardship to one of four security classifications: public, internal, sensitive and highly sensitive. These classifications are based upon the information's intended use and the expected impact if disclosed.

The [Data Oversight Committee](#), chaired by the Chief Information Officer (CIO), will publish, at a minimum, the following:

1. [Information Handling Standards](#)
2. [Security Configuration Standards](#)
3. [Server Management Standards](#)

These standards will specify controls to manage risks to the confidentiality, integrity and availability of University information and related assets. All individuals at the University are responsible for complying with these controls. The University will conduct periodic risk assessments to determine the effectiveness of such controls, and perform audits to measure levels of compliance. The [Data Oversight Committee](#) will review all standards related to this policy on a regular cycle that it determines to be appropriate.

The [Data Oversight Committee](#) will arbitrate disputes related to this policy. Appeals of [Data Oversight Committee](#) decisions can be made in writing to the Provost or Executive Vice President.

The Office of Information Technologies will maintain a formal information security awareness, training and education program, to ensure that all individuals are aware of their responsibilities.

The Office of General Counsel and Office of Information Technologies will review information technology product or service contracts. This review will include identification of risks related to information security.

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

| | |
|--------------------------------------|--|
| Data Handling | Using, storing, processing, transferring, administering, aggregating, sharing, and/or maintaining University information |
| Information Security | The protection of the confidentiality, integrity, and availability of University information. |
| Information Technology Assets | Applications, computer systems, servers, networks and related devices owned by or entrusted to the University. |
| Security Classifications | Categories of University information based upon intended use and expected impact if disclosed. |

Public

Information intended 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.

Internal

Information not intended for parties outside the University that, if disclosed, would have minimal or no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

Sensitive

Information intended for limited use within the University that, if disclosed, could be expected to have a serious adverse effect on

the operations, assets, or reputation of the University, or the University's obligations concerning information privacy.

Highly Sensitive

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

| | |
|-------------------------------|---|
| University Information | All information that the University of Notre Dame or its agents use in the course of conducting University business, except those materials specifically excluded from University ownership as set forth in the University's Intellectual Property Policy . |
| University Records | Recorded information, in any form, created or received in the course of conducting University business and kept as evidence of such activity, excluding transitory work products. |

5. RESPONSIBILITIES

| | |
|----------------------------------|---|
| Chief Information Officer | <ol style="list-style-type: none"> 1. Appoints members of the Data Oversight Committee. 2. Serves as the chair of the Data Oversight Committee. 3. Acts as Data Steward for all University information not otherwise assigned. |
| Data Oversight Committee | <ol style="list-style-type: none"> 1. Assigns responsibility for managing specific elements of University information to individual Data Stewards. 2. Approves information handling standards. 3. Recommends business process or control changes necessary for compliance with this policy. 4. Arbitrates disputes related to this policy or related standards. Appeals of Data Oversight Committee decisions can be made in writing to the Provost or Executive Vice President. 5. Ensures that the University conducts periodic risk assessments. 6. Conducts periodic review of all standards related to this policy. 7. Conducts annual review of this policy. |
| Data Steward | <ol style="list-style-type: none"> 1. Ensures the confidentiality, integrity and availability of University information for which assigned responsibility. 2. Classifies all University information for which assigned responsibility. 3. Defines access to and restrictions on use of the information for which he or she is responsible. |
| Faculty, Staff, Students | <ol style="list-style-type: none"> 1. Protect the privacy and security of University 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 or to the appropriate Data Steward. |

| | |
|---|---|
| Office of Information Technologies | <ol style="list-style-type: none"> 1. Implements this policy. 2. Maintains the information security awareness, training and education program. 3. Investigates suspected violations of the Information Security Policy. 4. Assists in creating and maintaining standards and procedures related to this policy. |
|---|---|

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 |
|---|---|
| Incident Response Policy and Procedures | http://oit.nd.edu/policies/itpolicies/incidentresponse.shtml |
| Information Handling Standards | http://oit.nd.edu/policies/itstandards/infohandling.shtml |
| Intellectual Property Policy | http://or.nd.edu/technology-transfer/for-faculty/intellectual-property-policy/ |
| Records Management and Archives Policy | http://policy.nd.edu/policy_files/RecordsManagementandArchivesPolicy.pdf |
| Responsible Use of Information Technologies at Notre Dame | http://oit.nd.edu/policies/rup.shtml |
| Security Configuration Standards | https://secure.nd.edu/standards/index.shtml |

| | |
|---|---|
| Server Management Baseline Standards | http://oit.nd.edu/policies/itstandards/servermanagement.shtml |
|---|---|

| | |
|-----------------------------|---|
| Strong Password Standard | http://oit.nd.edu/policies/itstandards/strongpassword.shtml |
|-----------------------------|---|

7.2.

External Documents Web Address

| | |
|---|---|
| Code of practice for information security management; ISO 17799 | http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612 |
|---|---|

| | |
|---|---|
| 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 | Telephone Number | E-mail |
|------------------------------|--------------------------------|---|--|
| Policy Content/Violations | OIT Information Security | (574) 631-5600 | infosec@nd.edu |
| Policy Process | OIT Policy Office | (574) 631-5600 | itpolicy@nd.edu |
| Web Address for this Policy | | http://policy.nd.edu/policy_files/InformationSecurityPolicy.pdf | |