Data Classification Guidelines and Procedures
Approved by Data Management Committee: 29 May 2015
Approved by Information Technology Steering Committee: 30 July 2015

1.0 Purpose

The purpose of these guidelines is to establish a framework for classifying institutional data based on its level of sensitivity, value and criticality to the University. Classification of data will aid in determining baseline security controls for the protection of data.

2.0 Scope

These guidelines apply to all Northern Illinois University (NIU) faculty, staff and third-party agents of the University, as well as other University affiliates, authorized to access Institutional Data to include paper documents or any form of media or digitally based data. In particular, these guidelines apply to Data Stewards, who are responsible for classifying and protecting Institutional Data.

3.0 Guidelines

It is the practice and intent of NIU to protect the confidentiality, integrity and availability of Institutional Data. This protection includes the activities to classify institutional data and apply business processes and enterprise architecture standards to ensure the confidentiality, integrity and availability of Institutional Data while maintaining suitable utility and access for university purposes.

Data classification also reflects the level of impact to the University if confidentiality, integrity or availability is compromised. If an appropriate data classification is not inherently obvious, the Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology shall be applied. (see appendix A for a sample classification schema).

Finally, it is the practice and intent of NIU to systematically and regularly review the classification of Institutional Data and validate related processes, policies and standards applied to Institutional Data.

3.1 Reclassification

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the University. This evaluation should be conducted by the appropriate Data Steward. Conducting an evaluation on an annual basis is encouraged; however, the University’s Data Management Committee (DMC) should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

3.2 Risk Assessment

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used.
3.3 Categories:

- **Confidentiality** is implemented by preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Availability** ensures timely and reliable access to and use of information.

<table>
<thead>
<tr>
<th>Category</th>
<th>RISK LEVEL: LOW</th>
<th>RISK LEVEL: MEDIUM</th>
<th>RISK LEVEL: HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Integrity</td>
<td>The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Availability</td>
<td>The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>

4.0 Enforcement

As designated by the President, the Chief Information Officer, or designee, has primary responsibility for the interpretation and enforcement of these guidelines.

5.0 Accountability

All forms and instances of data are required to be classified by the Data Steward in accordance with University guidelines and policies. All faculty, staff, and third-party agents are responsible to be aware of the data classification for which they have access or oversight and to apply appropriate and pre-determined safeguards. As the total potential impact to the University increases from low to high, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Information Security Office for assistance.

6.0 Procedure

Data Stewards shall apply the principles of confidentiality, integrity, and availability to the data classification process.
7.0 Definitions

- **Confidential Data**: A general term that typically represents data classified as Restricted.

- **Data Classification**: In the context of information security, data classification is based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:

  **Restricted Data**
  Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted data. Restricted data generally requires a high risk in one or more categories.

  **Private Data**
  Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. **By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data.** A reasonable level of security controls should be applied to Private data.

  **Public Data**
  Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data. Public data typically rates low in most or all risk categories.

- **Data Custodians**: Appointed by Data Trustees and often directly reporting to Data Trustees, Data Custodians are the subject matter experts of how data is defined and used and they understand the business processes surrounding the data. They enforce data policies and procedures within their business unit.

- **Data Management Committee (DMC)**: A subcommittee of the IT Steering Committee (ITSC) structure. The DMC is NIU’s governing authority for information management programs and provides support and advice regarding the administration, access and use of NIU data. The DMC works with NIU’s management and committees chartered to support the institution’s business processes. The DMC’s efforts focus on the roles and responsibilities for providing the required accountability, leadership/ownership and resources for the development and support of NIU’s strategic information management assets.

- **Data Steward**: A senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data.

- **Data Trustees**: University officials with authority to approve policies and procedures and make data usage and access decisions.

- **Institutional Data**: Any data owned, licensed, or collected by the University.
Appendix A: Predefined Types of Restricted Information

1. Authentication Verifier

An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to:

- Passwords
- Shared secrets
- Cryptographic private keys

2. Covered Financial Information

Refer to the University’s Gramm-Leach-Bliley policy and procedure.

3. Electronic Protected Health Information ("EPHI")

EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For the purpose of this definition, electronic media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks and the physical movement of removable and/or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

4. Export Controlled Materials

Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State. See the Information and Guidelines on Federal Export Control Laws and Regulations, published by the Office of Sponsored Programs, for more information.

5. Federal Tax Information ("FTI")

FTI is defined as any return, return information or taxpayer return information that is entrusted to the University by the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.

6. Payment Card Information

Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
7. **Personally Identifiable Education Records**

Personally Identifiable Education Records are described in the Family Educational Rights and Privacy Act (FERPA) of 1974 (20 USC §1232g) and are defined as any Education Records that contain one or more of the following personal identifiers:

- Name of the student
- Name of the student’s parent(s) or other family member(s)
- Social security number
- Student number
- A list of personal characteristics that would make the student’s identity easily traceable
- Any other information or identifier that would make the student’s identity easily traceable

8. **Personally Identifiable Information**

For the purpose of meeting security breach notification requirements, PII is defined as a person’s first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver’s license number
- State-issued identification card number
- Financial account number in combination with a security code, access code or password that would permit access to the account
- Medical and/or health insurance information

9. **Protected Health Information ("PHI")**

PHI is fully defined in the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR 160.103). In summary, PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium by a Covered Component, as defined in the Northern Illinois University HIPAA Policy.

PHI includes "demographic information collected from an individual . . . created or received by a health care provider, health plan, employer . . . [that] relates to . . . health or condition of an individual; the provision of health care to an individual . . . that identifies the individual or [provides] a reasonable basis [for identification]. PHI does not include education records or treatment records covered by the Family Educational Rights and Privacy Act or employment records held by the University in its role as an employer."