University Policy

Volume I1: Information Technology	**I1.99.1** **Data Governance** **Interim Policy**	**Responsible Office:** University Technology Services
Chapter 99: General	**Effective Date:** 06/21/2023 **Last Revised:** mm/dd/yy	**Responsible Officer:** Information Security Officer

POLICY STATEMENT

The University holds and processes various types of data to carry out its operations. It is essential that university data is assigned the appropriate sensitivity category and the minimum-security controls necessary to keep it safe from unauthorized or unintentional access, mishandling, or misuse.

PURPOSE OF THE POLICY

The purpose of this policy is to establish a data governance process to maintain the confidentiality and integrity of university data from the time of creation or collection to disposal.

WHO IS AFFECTED BY THIS POLICY

All university employees, students and third parties who hold, use, and process university data.

DEFINITIONS

Data Classification: The grouping of data into different sensitivity categories for the purpose of providing the appropriate security and privacy safeguards for each category.

Data Custodian: A person with daily management responsibility for the data under their purview. They are responsible for maintaining access to, accuracy, and completeness of data.

Data Owner: A person with the overall authority and decision-making responsibility over the data under their purview. This includes defining and creating data and the business rules for use of data.

System Owner: A person with the overall authority and decision-making responsibility over the information systems under their purview. They may also have the role of a data owner if the data stored is under their purview.

Data Sensitivity: This is the level of confidentiality a dataset should have and the severity of the impact on an organization or individual should data be breached.

Privacy Regulations: These are various privacy rules and requirements established by state and government bodies to safeguard the security and privacy of data held and processed by private and public organizations.

Data Breach: An incident that results in unauthorized access, modification, or deletion of data.

Impact Severity: This is the degree to which an event, e.g. a data breach, may impact an individual or organization.

Information Handling: These are the practices for handling data securely based on its sensitivity.

REGULATIONS

Data Classification

All data held and used by the university will be classified under the following (*see* Appendix A):

- Restricted
- Internal
- Public

These classifications are governed by various data privacy legislation which the university is required to comply with. These include the following:

Legislation

Identify Protection Act:

- This act sets out the requirements for protecting the confidentiality of Social Security Numbers (SSNs) by requiring state and government agencies to implement policies and procedures for maintaining the confidentiality and integrity of SSNs and to train employees who handle SSNs. Learn how the University complies with the act.

Family Educational Rights and Privacy Act (FERPA):

- The Family Educational Rights and Privacy Act (FERPA) protects access to and release of student records and gives students the right to know the information that is held about them and to request corrections to be made if the information is incorrect or misrepresented.
- Student information designated as Directory Information is not subject to FERPA and can be released by the University without the student's permission. Directory information includes name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance.
- The university has implemented a FERPA policy and guidelines for the release of student information.

Health Insurance Portability and Accountability Act (HIPAA):

- HIPAA sets out the requirements for maintaining the privacy of Protected Health Information (PHI).
- Any health information or record that can be traced to an individual is PHI. Identifiable health information includes:
  - Physical and mental health information about an individual in the past, present, or future.
  - Healthcare service information for the individual by a covered entity (for example, hospital or doctor) and payments of healthcare services provided to the individual in the past, present or future.

Gramm Leach Bliley Act (GLBA):

For higher education institutions, GLBA sets out the requirements for collecting, storing, and using student financial records containing personally identifiable information. Information relating to student loans and financial aid applications is protected by GLBA.

Payment Card Industry Data Security Standards (PCI DSS):

PCI DSS sets out the requirements to safeguard the privacy of payment card information or cardholder data. At a minimum, this type of data consists of the full PAN (primary account number) and may also appear in the form of the full PAN plus any of the following:

- Cardholder name
- Expiration date
- Service code

General Data Protection Regulation (GDPR):

GDPR defines personal data as data that can be used to identify an individual directly or indirectly using a single or multiple data sets. It sets out the requirements for collecting, using, processing, securing, and maintaining data privacy and integrity, and retaining and disposing of personal data. The data types covered in the GDPR encompass all the data types covered under the privacy regulations listed above, and other information such as international passport data, computer IP address and cookie information, vehicle registration number, resume data, location data, email address, and political data opinion.

Others:

Government classified data**,** driver's license details, biometric data, encryption keys, intellectual property data, research data, business proposals, etc. These types of information must not be disclosed without authorization/consent by the data owner.

Information Handling Requirements

For each classification group, there are security and privacy measures that set out the expectations and practices for handling data appropriately. **Where a record holds datasets that fall under different classifications, the most stringent handling requirements must apply.**

Roles and Responsibilities

Data Governance Group: This group is responsible for instituting and reviewing the data governance process, including identifying and defining data sensitivity categories and ensuring appropriate measures are established to safeguard university data and comply with privacy legislation.

The group is also responsible for reviewing exceptions to the application of this policy and providing guidelines on the implementation of such exceptions to ensure data privacy and integrity are maintained.

Group membership includes data and system owners or designees (data custodians), and a representative from each college and business unit.

Data and System Owners: They are responsible for ensuring that the confidentiality and integrity of data or systems under their control are maintained. They are also responsible for ensuring the data in their custody is assigned the right classification category and use of such data complies with the handling procedures.

It is important to note that the data handling requirements for each classification type are the minimum requirements for protecting related data. Some legislation may require additional privacy and security measures, and data or system owners are to consider the additional requirements where applicable and consult with the information security team for guidance.

Data Custodians: They are responsible for promoting and ensuring that the daily operation and management of data under their responsibility comply with the requirements of this policy and applicable legislation. This includes ensuring the right access, modification, storage, and transfer of data, and monitoring and auditing data handling.

Functional Users: are responsible for handling data in line with the security and privacy requirements for each data classification category. If unsure, please contact the data owner, custodian, or the information security team (uinfosec@neiu.edu) for guidance.

PROCEDURES

When embarking on a new project requiring the collection and processing of data, **data owners** should follow the procedure below to identify the data classification group and handling requirements:

- Determine the purpose for using the data type. That is, identify if this data is needed to implement the project or carry out the specified business operation.
- If yes, determine which data classification category the data falls under using the data classification table.
- Consider the impact of a breach of such data and implement the appropriate departmental privacy and security measures using the related data handling requirements and any additional measures defined by the governing regulation.

GUIDELINES

Data Usage and Risk Management

- Before collecting or creating data, consider if the data is appropriate for the business need in view of the governing legislation.
- When assessing the likelihood and impact level of a breach of such data, consider what data handling processes might easily be susceptible to a data breach and the legislative implications of a breach to the university and individuals, and determine which measures to implement to reduce the risk of a breach. For example, identify other alternative handling processes that may be less susceptible to a breach. Consult the information security team for advice at uinfosec@neiu.edu.
- To implement the departmental privacy or security measures to put in place, consider controls that will enhance data privacy (confidentiality) e.g. training for functional users or additional access controls such as multifactor authentication (MFA), etc.

Data Inventory

- Keep an inventory of the data you maintain, including the purpose, the data custodian, and other departments with access to such data.
- Consider including the following information in your data inventory to maintain the relevant details about the data:
  - System name and the type of data held
  - Classification group
  - Where data is hosted (internally or by a third party),
  - URL to the web application (if applicable)
  - Custodian contact,
  - Business units with access to the data.

APPENDIX

Appendix A. Data Classification Table and Information Handling Requirements

HISTORY

8/08/2023 – removed linked Data Classification Table and added it as Appendix A
6/21/2023 – Interim approval granted
6/07/2023 - Draft of policy submitted for interim approval

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

I1.02.5 Information Security Policy
I1.01.1 Acceptable Use of ITR Policy
I1.02.4 Identity Protection Policy
I1.02.8 Payment Card Industry Data Security Standard Policy

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	Email
Help Desk	(773) 442-4357	helpdesk@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.

APPENDIX A

Appendix A - Data Classification Table and Information Handling Requirements

Data Classification	Description	Examples	Handling Requirements
Restricted	• This type of information is governed by privacy laws, and contractual and legal agreements, sensitive business data, to protect the confidentiality and integrity of such information. • This type of data is high risk and requires the highest level of protection possible. • Inappropriate or unauthorized disclosure may cause severe damage or distress to an individual, impede the university's normal operations, and/or cause severe financial impact, litigation, or reputational damage to the university.	• Protected health information • Social security numbers • Protected education records • Financial records relating to students, employees, or the university. • Credit card information • Unpublished research plans and data • Intellectual property information • Government-protected information • Commercially sensitive university strategies or plans • Driver's license information • Biometric data, sexual orientation, felony records, etc. • System security information such as encryption keys, passwords, firewall rules, multifactor authentication codes, system configuration information, and test reports.	• Information requires stringent security controls to maintain its confidentiality and integrity. • Use: Check the statutory requirements and university policies for the use of such information. • Authorization: Obtain authorization from data owners before collection and use. • Collection limitation: Collect only what is needed for the intended work purpose. • Storing and Transmission: Use approved systems and secure methods for storing and sharing or transmitting data. • Retention: Follow the university's record retention policy or the retention agreement for the specified use. • Such information requires at the minimum, the security measures set out in the university's information security standard **and additional measures for storing, transmitting, sharing, processing, retaining, and disposing of data as required by the governing law, contractual or legal agreement.**

Internal	• This type of information is internal to the university and is not shared with third parties unless required by governing regulations, or legal agreements or authorized by data owners. • Inappropriate disclosure of such information may negatively impact an individual or the University's objectives and/or reputation.	• Information about individuals such as contracts and unpublished salaries, work performance reviews or assessments, employee or student IDs, job references, transcripts, coursework, test assessments and results, and contact details. • Information relating to disciplinary proceedings or investigations • Unpublished university financial and audit reports and other information that should only be disclosed to the public as required by law. • Contract information and agreements with third parties, and third-party audit reports. • Internal communications and documents. • Gifts and donors' information • Insurance information	• Use: Check the statutory requirements and university policies for the use of such information. • Authorization: Obtain authorization from data owners before collection and use. • Collection limitation: Collect only what is needed for the intended work purpose. • Storing and Transmission: Use approved systems and secure methods for storing and sharing or transmitting data. • Retention: Follow the university's record retention policy or the retention agreement for the specified use • Retention: Follow the university's record retention policy or the retention agreement for the specified use. • Such information requires at the minimum, the security measures set out in the university's information security standards.
Public	• Information that is not harmful or an invasion of privacy if made public. • Information is available in the public domain, such as the university's website, through search engines or government portals. • Information is available on social media platforms. • Disclosure has no negative impact on individuals or the university	• Policies, academic degrees and regulations, degree programs, and school events. Routinely published financial and audit reports, published strategies, published board meeting minutes, and announcements. • Directory information for employees and students.	• Such information must be kept up-to-date with restrictions for editing limited to authorized individuals. • It must be stored only in university-approved systems.