Policy Title: Data Classification
Policy Summary: Requirements for identification, classification, and handling of university data and information assets.
Policy Category: Information Technology Services (ITS)
Policy Owner: Information Technology Services (ITS)

Purpose

The purpose of this policy is to define the data classification requirements for information assets and to ensure that data is secured and handled according to its sensitivity and impact that theft, corruption, loss or exposure would have on the institution. This policy has been developed to assist Drake University (Drake) and provide direction to the institution regarding identification, classification, and handling of information assets.

Scope

The scope of this policy includes all information assets governed by Drake. All personnel and third parties who have access to or utilize information assets to process, store and/or transmit information for or on the behalf of Drake shall be subject to these requirements.

Policy

Roles and Responsibilities

Drake has assigned the following roles and responsibilities to ensure appropriate controls and procedures are in place and followed to protect the University's data and information assets:

- President's Council - possess authority and responsibility for the security, accuracy, and confidentiality of data within their areas of accountability. While President's Council members may delegate responsibility to Data Stewards or Custodians for the management of data (including granting inquiry, entry and update data privileges, maintaining and controlling Banner validation and rules tables, and defining business processes).

- Information Security Steering Committee (ISSC) – Responsible for monitoring the implementation of this policy and reporting to senior management on any abnormal findings or exceptions.

- Data Steward – responsible for planning, implementing and managing the creation, use and maintenance of data contained in specific Data Domains as assigned by the University. Data Stewards are responsible for Data Quality, integrity, and use within assigned Data Domains in the pursuit of effective decision-making. Data Stewards are commonly responsible for data content, context, and associated business rules surrounding the management and use

of institutional data.

- Data Custodian – manages the technical environment where data resides. Custodians ensure safe custody, transport, and storage of data. Typically, Data Stewards and Data Custodians work closely to ensure effective operational management of institutional data. While Data Stewards manage the data itself, Data Custodians manage the systems and infrastructure that support data creation, storage, access, and protection.

- Data User - institutional employee who performs activities on the institutional data and operates within the policies and guidelines created by the president's council and the ISSC.

- All Employees –
  - Responsible for classifying and marking all created or modified information, including any reproductions that are made (e.g. reports).
  - Responsible for appropriate handling of all classified information (electronic or non-electronic).

Data Classification

Classification of data will be performed by the data asset owner based on the specific, finite criteria. Refer to the Data Classification and Handling Procedure to determine how data should be classified. Data classifications are defined as follows:

1. RESTRICTED - Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial or reputational harm to the institution, institution staff or the constituents we serve. Federal or state breach notification would be required, identity or financial fraud, extreme revenue loss, or the unavailability of extremely critical systems or services would occur. Common examples include, but are not limited to,
   - Passwords
   - Social Security number
   - Credit card number
   - Driver's license number
   - Bank account number
   - Protected health information, as defined by the Health Insurance Portability and Accountability Act (HIPAA)
   - Student Records protected by the Family Educational Rights and Privacy Act (FERPA) requests for confidentiality

2. PRIVATE – Information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial or reputational harm to the institution, institution staff or the constituents we serve. Federal or state breach notification would not be required, limited identity theft and very little revenue loss would occur, and the availability of critical systems

would not be affected. Common examples include, but are not limited to, some data elements found in HR employment records, unpublished research data, and passport and visa numbers.

Student Information is considered PRIVATE and is defined as the following:

- Student's name, address (except residence hall room number), telephone number, and email address
- Parent's name, address and telephone number
- Date and place of student's birth
- College/school of enrollment
- Curriculum (major field of study)
- Year in school
- Participation in recognized organizations, activities and sports
- Weight and height of members of athletic teams
- Degrees and awards received (including names of Drake-funded scholarships)
- The most recent previous educational institution attended by the student
- Job title(s) and date(s) of employment held while enrolled as a student

3. PUBLIC – Information whose loss, corruption, or unauthorized disclosure would cause minimal or no personal, financial or reputational harm to the institution, institution staff or the constituents we serve. Common examples include, but are not limited sales and marketing strategies, promotional information, published research data, and policies.

4. DIRECTORY INFORMATION
   Workforce Information is defined as the following:
   - Name
   - Current position title
   - Department of assignment, including office telephone number and office address

Re-classification

A re-evaluation of classified data assets will be performed periodically by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired or destroyed.

Classification Inheritance

Logical or physical assets that "contain" a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

Access

Data Custodians are responsible for ensuring all workforce are provisioned with appropriate access to information and information systems. Access to information and information systems will be provisioned on a least privileged basis. Banner Access Control Procedures must be followed should additional access be required to perform job functions.

Enforcement

Users who violate this policy may be denied access to the institution's resources and may be subject to penalties and disciplinary action both within and outside of the institution. The institution may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it appears reasonably necessary to do so in order to protect the integrity, security or functionality of the institution or other computing resources or to protect the institution from liability.

Exceptions

Exceptions to this policy must be approved in advance by the Chief Information Technology Officer, at the request of the responsible data asset owner. Approved exceptions must be reviewed and re-approved by the asset owner annually.

References

- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-171, 800-53

Last Review Date: July 2024
Effective Date: June 2023