

Duke University Standard: Data Classification

University IT Security Office

Version 2.1

Authority:

Duke University Chief Information Officer

Duke University Chief Information Security Officer

1. Definitions

Term	Definition
Data Owner	The owner of an information or data element. The Data Owner is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information.
Data Manager	The persons who are responsible for implementing the controls the owner identifies.
Data Users	The persons who actually "touch" the information (enter, delete, even read).
High Risk	A High Risk impact is an event that would cause severe and long-term interference with the mission of the University or a business unit, or would result in major financial loss, or would result in severe harm to an individual's life or livelihood.
Moderate Risk	A Moderate Risk impact is an event that would cause significant interference with the mission of the University or business unit, result in significant financial loss; or result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low Risk	A Low Risk impact is an event that would cause some interference with the mission of the University or business unit or result in minor harm to an individuals well being.

2. Purpose

While performing their assignments at Duke University, all users will likely come into contact with many types of information or data, some of which may be considered Sensitive or Restricted according to Duke's data classifications and regulatory requirements. It is the responsibility of Duke to implement procedures and standards to help users protect their data.

The purpose of this standard is to define Duke's data classifications and data types for each classification. Please be aware that applicable federal and state statutes and regulations that guarantee either protection or accessibility of certain data records will take precedence over this standard. These regulations and laws include:

- FERPA (which protects many kinds of student educational data)
- HIPAA (which protects personal health information)
- HHS Title 45 CFR Part 46 - Protection of Human Subjects (which applies to research supported by a federal agency)
- NC GS 125-19 (which protects the privacy of library patrons' records)
- NC Identity Theft Prevention Act (which defines personal information and requires notification if a data breach occurs)
- PCI (which protects credit card holder information)

3. Scope

This standard applies to all data collected, stored, or processed by university staff or by third parties via contractual agreements with university departments or other organizational groups.

4. Standards

4.1 Data and Risk Classifications

To assist in determining how to talk about handling information in any format, Duke has defined three classes of information: Sensitive, Restricted, and Public. Each classification tier requires a specific level of technical and procedural security controls due to the risk impact if the information is mishandled. These Technical Standards may be found at <http://security.duke.edu>.

Data that has not yet been classified should be considered Restricted until the Owner assigns the classification.

The classification of data is independent of its format. For example, if personal health information is revealed in a video recording of a lecture, then that video file should be classified as Sensitive. If paper credit card receipts are stored, then they should be classified as Sensitive.

Questions about classifying or handling the data should be directed to the Data Owner, your supervisor, your departmental security liaison, or the University IT Security Office. The departmental security liaisons, in coordination with the IT Security Office, can assist departmental users in developing appropriate controls and processes to protect Sensitive or Restricted data.

Data Category & Risk	Definition & Access	Examples
Sensitive (High)	<p>Sensitive data is the most restrictive data classification category and is reserved for data that Duke is either required by law to protect, or which Duke protects to mitigate institutional risk. Explicit institutional approval is needed in order to receive access to Sensitive data.</p>	<ul style="list-style-type: none"> • Social Security numbers • Credit Card numbers • ePHI (HIPAA –protected data) • FERPA-protected data (non-directory information) • Prospective student data • Donor data • Contract data • Financial data • HR data • Physical Plant details • Certain management information
Restricted (Medium)	<p>Restricted information is the default data classification category. Restricted data is data that is not necessarily for public consumption, but also does not fit into the Sensitive category. Duke may have a proprietary obligation to protect Restricted data, but disclosure would not significantly harm the university. Access to Restricted data elements is determined by business process needs.</p>	<ul style="list-style-type: none"> • Anything not Public or Sensitive • Data that is restricted to specific groups • Research detail that is not classified as Public or Sensitive • Library transactions • Financial transactions not including Sensitive data • NDA data
Public (Low)	<p>All other data, which can be accessible to the general public. Information that has been approved for publication, such as a press release or information published on www.duke.edu. (This does not include information that has been disclosed accidentally.) Access includes Duke University affiliates and general public.</p>	<ul style="list-style-type: none"> • Public-facing websites • Campus maps • FERPA directory data • Faculty/Staff directory data

4.2 Roles and Responsibilities

To handle data properly, Duke faculty and staff need to be aware of the classification of a piece of information and the associated risks in order to understand how to properly and securely handle the information.

Role	Responsibility
Owner	The owner of an information element. The Data Owner is the role of the person who is responsible for: the function that uses the information, determining the levels of protection for the information, making decisions about appropriate use of the information, classifying the information, and for the business results of the system or the business use of the information.
Manager	The persons who are responsible for implementing the controls the owner identifies. The data managers are responsible for ensuring that the appropriate security controls are in place on systems containing Sensitive and Restricted data (see Technical standards).
User	The persons who actually "touch" the information (enter, delete, even read). Users are responsible for taking reasonable precautions against disclosure of data they have access to. Users should not grant access to data without proper authorizations from the Data Owner.
Campus Units	It is the recommendation of the University IT Security Office that all campus units that collect and store information <u>document</u> their policies, procedures, and architectures that pertain to collection and storage, regardless of the information format (electronic, paper, image, sound, etc.). This documentation should detail account creation and deletion, records retention and destruction, backup retention and destruction, and any other relevant procedures.

4.3 Sensitive Server Registration

The University IT Security Office tracks servers containing Sensitive data. Campus units are asked to document which of their servers contain Sensitive and Restricted data, and update the ITSO on which systems contain Sensitive information.

4.3 Incident Reporting

Report the misuse or compromise of systems that handle, store or propagate Sensitive data IMMEDIATELY to security@duke.edu.

Review Frequency: Annually

Updated: 5/11

In Compliance with:

Duke University Technical Standards

Duke University Acceptable Use Policy