DOANE

Data Classification

Purpose

The purpose of this policy is to provide clear guidelines and procedures to ensure Doane University understands and protects information for the benefit of the university and its constituents.

Scope

This policy applies to all employees who interact with Doane University Data. The Chief Information Officer is responsible for coordinating the university's response to any violation of this policy to ensure prompt action, mitigate risk, and maintain compliance with applicable regulations and contractual obligations.

Policy

All data at Doane University is classified into one of the following categories. By default, all data is considered Level 2 - Internal, unless otherwise specified. Data containing a combination of data sets is classified at the highest classification level unless otherwise specified.

"Doane enterprise systems" includes, but is not limited to, Salesforce, Colleague, Canvas, Google Drive (with appropriate, restricted access), and other third-party tools explicitly approved by Technology Services to contain Doane data.

Level 1 - Public

Public data includes data that is purposely designed to be shared freely and would not cause potential harm to the university. Data is typically presented in aggregate, available through other means, or required to be displayed publicly by law or regulation. May include information that is shareable upon request.

Examples: Advertising, public disclosure websites, approved employee directory information, published research findings.

Data Use: No restrictions on use or storage.

Level 2 - Internal

Internal data refers to information that is not publicly available without appropriate prior authorization. The release of Internal data may have a negative impact on the university, but would not result in financial loss or legal liability.

Examples: University ID numbers, personal cell phone numbers, email, internal chats

Data Use: Information may be sent via email or any other approved Doane communication medium (Zoom, gChat, Netfiles, Google Drive, etc.)

Level 3 - Confidential

Confidential data refers to information for which disclosure could cause a moderate risk to University operations, employees, or students.

Examples: Employee home address, student data restricted by FERPA, research data, gift (donor) information

Data Use: Data typically remains on approved enterprise systems.

Level 4 - Highly Restricted

High Restricted data includes all information that must be protected to comply with legal requirements and contractual obligations, or if the disclosure would pose a significant risk to University operations, employees, or students.

Examples: Social Security Numbers, credit card numbers, IT infrastructure, HIPAA, FAFSA data

Data Use: Data should be maintained only on approved enterprise systems. Any use of data on individual university devices (laptops) must be temporary and deleted after use.

Data Examples Across Domains

Domain	Highly restricted	Confidential	Internal	Public
Student	Banking information	Grades	Registration	Dean’s list

Human Resources	Banking information, Insurance	Home address	Offer letter	Email, degrees
Facilities		Emergency management plans	Floor plans	Campus map

Violations

All violations of this policy must be reported to the Chief Information Officer via email at cio@doane.edu. The Chief Information Officer serves as the primary point of contact to ensure an immediate and coordinated response to potential risks affecting university data, systems, or operations. The Chief Information Officer will initiate the appropriate response and, when applicable, notify the Chair of the Data Governance Committee for policy oversight and review. Depending on the nature of the violation, the Chief Information Officer may also involve the General Counsel, Human Resources, Registrar's Office, or other relevant university offices to ensure proper investigation and resolution.

Updates

1. Draft created by Kris Williams 5/5/2025
2. Reviewed by Data Governance Committee 7/1/2025
3. Finalized by DGC 9/5/2025
4. Sent to ESC 11/14/2025
5. Requested meetings with Faculty Council, Staff Council, Dean's Council per Shared Governance 11/21/2025
6. Met with Faculty Council, Staff Council, Dean's Council, January - March 2026.
7. Approved by Leadership Team 4/14/2026.

Works consulted:

1. ECU Data Governance
2. UW - Madison
3. IU