Categorizing and Securing Institutional Data

Data Classification is the establishment of an enterprise framework for organizing, categorizing and securing data from the time it is created until it is destroyed, according to its level of risk, data type and criticality in the running of university business. In order to protect university data by complying with laws, regulations and standards, and to safeguard privacy and security, the university has developed an official model, as displayed in the matrix below, the Data Classification Guidelines (Guidelines).

Data Classification Guidelines

Risk Level	Risk Level Definition	Data Type Definition	Examples
Critical Risk Level 🔒🔒🔒🔒	Unauthorized public disclosure, alteration, or loss of this data would result in criminal or civil penalties, identity theft, financial loss, invasion of privacy and will have serious adverse effects on the University's reputation, resources, services or individuals.	Data that the university must keep private under federal, state, local or international laws and regulations, industry standards, and/or confidentiality agreements.	• Social Security Numbers • Credit Card Numbers • Medical Records • Passwords
High Risk Level 🔒🔒🔒	Unauthorized public disclosure, alteration, or loss of this data would adversely affect the University's missions, reputation, services, safety, finances, resources or individuals.	Data that is not for public consumption. Its handling is based on university-wide policy and/or internal procedures, and takes into account proprietary, ethical, business practice or privacy implications.	• Photos • Non-Directory Student Data • Employee Salary & Evaluations • Unpublished strategic and financial plans
Limited Risk Level 🔒🔒	Unauthorized public disclosure or loss of this data would not cause material harm and is unlikely to, but could, pose risk to the University's mission, reputation, services, resources and individuals.	Data that the university could publish by laws and regulations but has chosen to keep confidential. Its handling is based on university or department/unit protocols or procedures.	• Internal memos, reports • Internal operating procedures • Budget plans
No Risk Level 🔓	Public disclosure or loss of this data poses no risk to the University's mission, reputation, services, safety, finances, resources and individuals.	Data that may, or must, be available and accessible to the general public with no expectation for privacy, risk or confidentiality. There are no legal and institutional limitations on its access or use.	• Campus maps • Course Catalogs • FERPA Directory information (except for students who have requested non-disclosure)

Click here for an interactive companion tool to this matrix to help manage data at different phases of its lifecycle.