

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.	Unauthorized disclosure would cause <u>serious harm</u> , so it is required to be kept <u>strictly confidential</u> . Its handling is likely subject to legal restrictions and is governed by university policies, internal procedures & business practice requirements.	<ul style="list-style-type: none"> • 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.	Unauthorized disclosure of this data would cause <u>material harm</u> , so it is required to be kept <u>confidential</u> . Its handling may be subject to legal restrictions and is governed by university policies, internal procedures & business practice requirements.	<ul style="list-style-type: none"> • Non-Directory Student Data • Employee Salary & Evaluations • Unpublished strategic and financial plans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 <u>is unlikely to, but could, pose risk</u> to the University's mission, reputation, services, resources and individuals.	Unauthorized disclosure of this data may cause <u>harm</u> to the university so the university has chosen to keep it <u>confidential</u> . Its handling is governed by university or department/unit protocols or procedures.	<ul style="list-style-type: none"> • Internal memos, reports • Internal operating procedures
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 be made available and accessible to the general public without impacting confidentiality. There are no legal and institutional limitations on its access or use.	<ul style="list-style-type: none"> • Campus maps • Course Catalogs • FERPA Directory information (except for students who have requested non-disclosure)

This matrix above should be used on an educational basis only at this time. [Click here](#) for an interactive companion tool to this matrix to help manage data at different phases of its lifecycle.