

Information System Classification Standard

(OAR 580-055-0050-2A)

This standard provides guidance and policy standards regarding the classification of information systems to ensure the protection of EOU from accidental or intentional unauthorized access, damage, alteration or disclosure while preserving authorized users' ability to access and use institutional information. Institutional information is defined as all information created, collected, maintained, recorded or managed by the University, its staff, and all agents working on its behalf.

This standard applies regardless of the media on which data resides, for example electronic, microfiche, paper, CD\DVD, or other media. It also applies regardless of the form the information may take, for example text, graphics, video or audio, or their presentation.

This standard applies to all university constituents, whether students, faculty, staff, volunteers, contractors, affiliates, or agents, who have access to University information systems.

Unrestricted Information:

Unrestricted Information, while subject to University disclosure rules, may be made available to members of the University community and to individuals and entities external to the University. In some cases, general public access to Unrestricted Information is required by law.

While the requirements for protection of Unrestricted Information are considerably less than for Protected or Sensitive Information, sufficient protection will be applied to prevent unauthorized modification of such information.

Examples: Publicly posted press releases
High-level enrollment statistics
Course catalog
Financial statements

Sensitive Information:

Sensitive Information is information that must be guarded due to proprietary, ethical, privacy considerations. Its unauthorized access, modification or loss could seriously or adversely affect the University, its partners, or the public. High or moderate levels of restriction apply, both internally and externally, due to the potential risk or harm that may result from disclosure or inappropriate use. This classification applies even though there may not be a statute, rule, regulation, University policy, or contractual language prohibiting its release.

Sensitive Information must be protected from unauthorized access, modification, transmission, storage or other use. Sensitive Information is generally available to

members of the University community who have a legitimate purpose for accessing such information. Disclosure to parties outside of the University must be authorized by the appropriate department or unit head.

Examples: Research data where the corresponding research is incomplete
Responses to a Request for Proposal before decision is reached
Financial transactions
Library transactions

Protected Information:

Protected Information is information protected by statutes, rules, regulations, University policies, contractual language, and/or is considered to be personally identifiable. The highest levels of restriction apply, both internally and externally, due to the potential risk or harm that may result from disclosure or inappropriate use.

Protected Information must be protected from unauthorized access, modification, transmission, storage or other use.

Protected Information may be disclosed to individuals on a need-to-know basis within the University only. Disclosure to parties outside the University is generally not permitted and must be authorized by the appropriate Data Steward or University leadership.

Examples: FERPA – protected student information
Employee data and certain personnel documents/records
Prospective student data
Credit card numbers
Purchasing card numbers
Human subject information
Lab animal care information
HIPAA – protected health information