

8.2.1 Classification of Institutional Information and IT Resources

This policy addresses Institutional Information in electronic form. Other considerations may apply, including records management and privacy policies, and protection of paper records.

Proprietors must determine the Protection Level, summarized in the tables below, for Institutional Information and IT Resources under their area of responsibility.

Unit Information Security Leads and Proprietors must classify the Availability Level, summarized in the tables below, of Institutional Information and IT Resources under their area of responsibility.

Proprietors must comply with the UC Institutional Information and IT Resource Classification Standard.

Protection Levels and Availability Levels are used to select the security controls required by this policy and to drive key processes such as risk management.

Protection Level classifications:

Protection Level Classification	
Level	Impact of disclosure or compromise
P4 - High	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in significant fines, penalties, regulatory action, or civil or criminal violations. Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to: the risk of significant harm or impairment to UC students, patients, research subjects, employees, guests/program participants, UC reputation, the overall operation of the Location or essential services. (Statutory.)

P3 - Moderate	Institutional Information and related IT Resources whose unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Institutional Information of which unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss; or could require legal action. This classification level also includes lower risk items that, when combined, represent increased risk. (Proprietary.)
P2 - Low	Institutional Information and related IT Resources that may not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access. In addition, information of which unauthorized use, access, disclosure, acquisition, modification or loss could result in minor damage or small financial loss, or cause minor impact on the privacy of an individual or group. (Internal.)
P1 - Minimal	Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources for which the application of minimum security requirements is sufficient. (Public.)

Availability Level classifications:

Availability Level Classification	
Level	Impact of loss of availability or service

A4 - High	Loss of availability would result in major impairment to the overall operation of the Location and/or essential services, and/or cause significant financial losses. IT Resources that are required by statutory, regulatory and legal obligations are major drivers for this risk level.
A3 - Moderate	Loss of availability would result in moderate financial losses and/or reduced customer service.
A2 - Low	Loss of availability may cause minor losses or inefficiencies.
A1 - Minimal	Loss of availability poses minimal impact or financial losses.

8.2.2 Labelling of information

Units must identify Institutional Information and/or IT Resources under their control that require electronic or physical labeling.

8.2.3 Periodic review of classification

Units must review classification of Institutional Information and IT Resources periodically or when major changes occur.