



UNIVERSITY POLICY STATEMENT

UPS 103.004

COMPUTING RESOURCES USE POLICY

The computing resources at California State University, Fullerton (CSUF) are provided for the use of students, staff, faculty, consultants, auxiliary users, and contractors in support of the mission, goals and programs of the University. As a comprehensive university, CSUF, encourages the use of these resources for the free exchange of ideas and information among all members of the campus community and with members of other institutions. In this spirit, the Division of Information Technology (IT) seeks to ensure access (as determined by authorized University representatives) to computing resources (including Internet, intranet, software, hardware, user accounts, and all relevant cloud-based services and applications), unless they have been deemed to be in violation of applicable law or are judged to be detrimental to the security or proper functioning of the network and systems. These computing resources are the property of the University. IT has the responsibility to establish and publicize appropriate access, process priorities, resource usage, and security guidelines. Access is not transferable. In many instances, IT does not have control over updates to external computing resources (e.g., software, Internet, etc.).

UPS 103.004 is supplemental to CSU Systemwide policies including but not limited to Information Security Policy, Information Security of Personal Information Policy, Information Security Responsible Use Policy. Major changes to UPS 103.004 shall be reviewed by the Academic Senate Academic Technology and Library Committee and communicated to the campus community.

All users are required to adhere to this policy and CSU policies regarding but not limited to security policy and standards, responsible use, security of personal information, and student conduct. Adherence to professional ethics and standards, and engaging in responsible use of the resources including the honoring of license agreements, copyright laws, and file confidentiality is expected.

Any actual or suspected violation of these policies should be brought to the attention of the system administrator of the equipment or facility most directly involved. Violation of these guidelines may result in temporary loss of user privileges or user account. User consultation and notification shall be sought regarding loss of privileges. Violations will be dealt with in the same manner as violations of other University policies and may result in disciplinary review.

The following statements constitute University policy on computing resources; departments may specify additional guidelines as necessary.

1. User accounts are assigned for the individual use of a faculty, staff or student, and each is responsible for the proper use of this account. In line with CSU Responsible Use Policy (item 3.8), “other than publicly designated official CSU sites, the CSU does not generally monitor or restrict content residing on CSU systems or transported across its networks; however, the CSU reserves the right to use appropriate means to safeguard its data, preserve network, and information system integrity, and ensure continued delivery

of services to users. These activities are not intended to restrict, monitor, or use the content of legitimate academic and organizational communications.” This includes on- and off-campus use of CSUF computing resources.

2. Users are required to use and access computing resources only for the purposes for which they were assigned including, but not limited to, supervised cybersecurity research, instructional exercises, or formally authorized activity. Activities will not be considered misuse when authorized by appropriate University officials for security or performance testing.
3. When possible, users will be provided the choice to opt in for access to computing resources.
4. Violations of this policy include but are not limited to negligent or intentional conduct that leads to degradation of systems or performance of the network, deprivation of authorized personnel to resources or access to any University computer system, or gains unauthorized access to system resources. Knowledge of such violations by another user should be immediately reported to the system administrator of the equipment or facility most directly involved.

Source: Academic Technology and Library Committee

EFFECTIVE DATE: March 16, 2026
Supersedes: UPS 103.004 dated 10-22-2010
and ASD 15-05