

**POLICIES OF THE COLORADO STATE UNIVERSITY SYSTEM
POLICY FOR ALL INSTITUTIONS**

Acceptable Use Policy (AUP)	Effective Date: October 1, 2020
CSUS_CIO@Colostate.edu	

PURPOSE OF THIS POLICY

Computing and data systems, equipment and services at the Institutions of the Colorado State University System (each an “Institution,” or together the “Institutions”) are valuable and limited resources that serve a large number and variety of Users. Misuse of these resources can result in loss of integrity, functionality, speed, bandwidth and reliability of an Institution’s information systems, as well as violations of other laws and policies (such as those concerning conflicts of interest, privacy, etc.). The purpose of this policy is to establish what constitutes acceptable use of these resources in order to assure that they are available to everyone as needed for an Institution’s business needs.

APPLICATION OF THIS POLICY

This policy applies to all students, faculty and staff, affiliates, and all other persons and organizational units having access to technology and information systems deployed, offered by and/or contracted by an Institution (“Users”).

DEFINITIONS USED IN THIS POLICY

“Resources” include, but are not limited to, Institutional technology devices, servers, networks, storage devices and systems (including cloud storage), data, applications, installed software, and system credentials.

POLICY STATEMENT

All Users have the responsibility to make use of the Resources in an efficient, ethical, and legal manner. The Resources are to be used in a manner consistent with the instructional, research, and administrative objectives of the Institution in general, and for the purposes such Resources were provided. Access to the Resources is a privilege and imposes upon Users certain responsibilities and obligations, as further described in this policy.

POLICY PROVISIONS

Access to the Resources is granted subject to CSU System and Institutional policies and local, state, and federal laws. Acceptable use is always ethical, reflects academic honesty, integrity, and shows restraint in the consumption of shared Resources. It demonstrates respect for intellectual property, protection of sensitive information, ownership of data/information,

copyright laws, system security mechanisms, and an individual's rights to privacy and to freedom from intimidation and harassment. Activities inconsistent with these objectives are inappropriate and may jeopardize continued use of the Resources. An Institution may take any action it deems necessary to protect the Resources from systems and events that threaten or degrade operations, or that otherwise violate this policy, including the review of a User's actions or use of Resources.

In consideration of being allowed to use the Resources, each User acknowledges and agrees to the following statements:

- a. I will not use the Resources for any illegal activity or for any activity prohibited by this policy or the other policies or strictures referenced herein.
- b. I will not use the Resources to infringe upon any copyright or other intellectual property rights of another. This pertains to all copyrighted material, including, but not limited to, written works, recorded music, photographs, video and software. I understand that I may be held personally liable for copyright infringement. (See References below for more information on copyright laws and policies).
- c. I understand that I am responsible for my own misuse of the Resources, and misuse by others that I knowingly permit or enable to use the Resources (for example, by sharing my password or sharing my access). I agree to be responsible for all claims arising from my misuse of the Resources and shall indemnify and hold harmless the Board of Governors and the Institution from any costs, expenses and liabilities that might be asserted or imposed upon it or any of its officers, agents or affiliates as a result of such misuse.
- d. I will avoid any action that interferes with the efficient operation of the Resources or impedes the flow of information necessary for academic or administrative operations of the Institution and will immediately discontinue such activities once I become aware of its effects.
- e. I will protect the Resources from unauthorized use and acknowledge that I am responsible for reasonably securing the Resources that have been assigned to me, including implementing such measures as outlined within my Institution's IT Security Policy and any related procedures and guidelines, as well as in federal and state regulations that may apply (such as FERPA and HIPAA). This also includes applying, in a timely manner, operating system and software patches, and implementing malware scanning that protects my computing devices from unauthorized access.
- f. I will only use the Resources for their intended purposes. I will only access Resources that have been authorized for my use, or which are publicly available.
- g. I understand that the Institution retains ownership rights to all its collective data. I acknowledge that, unless specifically authorized by an Institutional official, copying Institutional data to a personal device, storage location or any other media, network or resource which is beyond the Institution's direct control is prohibited.
- h. I understand that incidental personal use of Resources (such as email, Internet access, fax machines, printers, and copiers) is permitted only when it conforms to this policy. "Incidental use" is use that is infrequent, does not interfere with the normal performance of my duties or the duties of another, does not unduly delay others' use, and does not cause the Institution to incur additional costs. Such use is restricted to

approved Users only and does not include family members or others not affiliated with the Institution.

- i. Storage of personal email messages, voice messages, files and documents on the Institution's Resources must be nominal so as not to burden the Institution's servers and other storage devices.

Examples of Inappropriate Conduct Using Institutional Resources

Conduct which violates this policy includes, but is not limited to:

- a. Accessing another person's computer, computer account, files, or data without permission.
- b. Giving my username and password to someone else, or allowing another to access my services, even temporarily.
- c. Using the Resources to gain unauthorized access to any computer system.
- d. Using any means to decode or otherwise obtain restricted passwords or access-controlled information.
- e. Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system.
- f. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses or malware, disrupting services, damaging files or making unauthorized modifications to Institutional data.
- g. Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.
- h. Making or using illegal copies of copyrighted software, storing such copies on Institutional systems, or transmitting them over Institutional networks.
- i. Harassing or intimidating others via email, social media, news groups or Web pages or any other of the Resources.
- j. Initiating or propagating electronic chain letters.
- k. Initiating or facilitating in any way mass unsolicited or unofficial electronic mailing (e.g., "spamming", "flooding", or "bombing").
- l. Forging the identity of a User or Resource.
- m. Saturating a Resource to the exclusion of another's use, for example, overloading the network with traffic such as emails, legitimate activities such as file backups, or malicious (denial of service attack) activities.
- n. Using the Institution's systems or networks for personal gain; for example, by selling access to your electronic identity or to Institutional systems or networks, or by performing work for profit with Institutional resources in a manner not authorized by the Institution.
- o. Engaging in any other activity that does not comply with the general principles presented above or are a violation of any other policies of the Board of Governors.

COMPLIANCE WITH THIS POLICY

The Institution considers violations of acceptable use principles or guidelines to be serious offenses. The Institution will take such action it deems necessary to access and examine any

files or information resident on Institutional systems allegedly related to unacceptable use, and to protect its network and resources from systems and events which threaten or degrade operations. Violations may be referred to the appropriate Institutional entity for disciplinary action.

In the case of major infractions, for example those that impair others' ability to use networking and computing resources, those that are a safety concern, or whenever necessary to protect Resources, the Institution may immediately restrict systems or network access as it deems necessary to mitigate such activities.

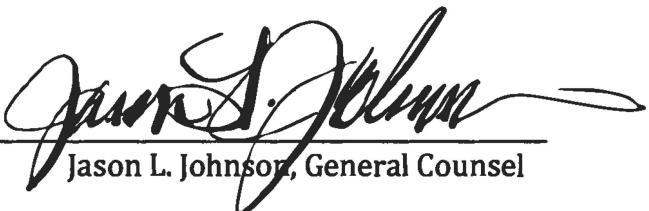
APPROVALS

COLORADO STATE UNIVERSITY SYSTEM

By: 
Anthony A. Frank, Chancellor

Date: 10/1/20

LEGAL REVIEW


Jason L. Johnson, General Counsel