Status Active PolicyStat ID 7983703

Origination	7/1/1999
Last Approved	9/7/2016
Effective	9/7/2016
Last Revised	9/7/2016
Next Review	6/1/2022

Area	Finance & Administrative Services (FAS)

Acceptable Use of Information Technology Resources

POLICY

Definition

The CSUSM information technology resources are a continually growing and changing collection of computers, networks, applications and services that supports the campus mission. These resources are vital for the fulfillment of the academic, research and business needs of the campus. To ensure a reasonable and dependable level of service, it is essential that each individual exercise responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt campus business, and the legitimate academic and research work of faculty and students. This document is intended to establish the acceptable use of CSUSM information technology resources.

Authority

CSUSM President

Scope

This policy is intended to apply broadly to individuals who access CSUSM information technology resources. These persons may be employees, students, volunteers, contractors, consultants, guests or others who have been issued campus credentials for purposes related to the campus mission.

Campus technology resources" may be campus computers or other devices or network, or use of the campus network via non-campus owned computer or device, or use of a hosted "cloud" application or resource which is used to support the campus

I. **BACKGROUND**

   A. This policy exists within a framework of state and federal laws, along with CSU and campus policies that may be related to the use of technology. The CSU has published a system-wide policy, "8105.0 Responsible Use Policy[1]" which applies broadly to all members of the campus community. Where an existing law or policy applies to an activity that may be conducted via or stem from the use of technology, that existing law or policy will be observed in conjunction with this policy.

B. This policy is intended to address those acceptable use issues which may expose the campus to liability due to violations of state or federal laws, or to civil claims, and to assure the effective and efficient use of information technology resources.

C. The CSUSM information technology resources are a continually growing and changing collection of computers, networks, applications and services that supports the campus mission. These resources are vital for the fulfillment of the academic, research and business needs of the campus. To ensure a reasonable and dependable level of service, it is essential that each individual exercise responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt campus business, and the legitimate academic and research work of faculty and students. This document is intended to establish the acceptable use of CSUSM information technology resources.

D. "Campus technology resources" may be campus computers or other devices or network, or use of the campus network via non-campus owned computer or device, or use of a hosted "cloud" application or resource which is used to support the campus mission.

II. Policy

A. It is the policy of the CSU to use any and all information technologies in a manner consistent with the federal laws governing copyright protection. These include, but are not limited to, the Digital Millennium Copyright Act of 1998, the Teach Act of 2002 and all subsequent amendments. Updated information about such laws can be found at http://www.copyright.gov/title17/.

B. This policy is intended to apply broadly to individuals who access CSUSM information technology resources. These persons may be employees, students, volunteers, contractors, consultants, guests or others who have been issued campus credentials for purposes related to the campus mission.

C. Privacy of Electronic Information

1. CSUSM supports each individual user's right to privacy and will take reasonable steps to ensure the security of CSUSM information technology resources. However, electronic messages, electronic files and electronic data residing on campus technology resources are potentially accessible to others through normal system administration activities or troubleshooting, in response to subpoenas or other court orders, and to the public through public records laws. Hence, the absolute privacy of electronic communication cannot be guaranteed. All users of CSUSM information technology resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or restricted access to such information.

2. The consent of an electronic communication holder or account owner

shall be obtained prior to the inspection, capture or disclosure of the contents of electronic communication records except as provided in paragraph II(C)(3).

3. CSUSM may inspect, capture, lock, or disclose of electronic communications records without the consent of the holder of such records or the owner of the account:
    a. *when required by and consistent with the law;*
    b. *when there is a substantiated reason to believe that violations of law, or policy, have taken place;*
    c. *when there are compelling circumstances that limit the ability of the record holder to give permission; or*
    d. *under time-dependent, critical operational or security-related circumstances.*

D. Protecting the Confidentiality of Electronic Information

1. Information stored on campus technology resources is subject to laws and/or policies related to confidentiality, privacy and intellectual property. Persons who store or access such information must use due diligence to prevent unauthorized access to and disclosure of confidential, private or sensitive information.
2. Due to the increasing legal requirements addressing protection of confidential information, files containing such information must be stored only on authorized systems in a secure manner. Individuals shall not store information on non-campus technology resources (i.e. computers, devices, services, and personal storage media) or otherwise make copies of sensitive or confidential information without express prior authorization of the CSUSM Information Security Officer.
3. Persons who use a personal computer or device (i.e. phone, tablet) to access a campus resources such as email or data storage service will be required to consent to the campus capability to enforce passcode/password unlock and/or "remote wipe" the device.[2]
4. Digital copies or backups of confidential data shall be stored in a secure manner. Individuals who create backups or copies of sensitive or confidential data shall store such backups or copies in an encrypted format where the decryption credentials are adequately secured and protected; preferably in a centralized management system.
5. Confidential or sensitive data in digital format must be thoroughly eliminated from computing equipment when no longer needed and/or prior to disposing of the equipment.

E. Legal Use of Equipment

1. Users shall not use CSUSM technology resources for purposes that are inconsistent, incompatible, violate or are in conflict with federal, state laws, as well as campus and CSU regulations and policies. Violations may

include but are not limited to harassment, defamation, making threats, committing computer-related crimes, impermissible use of campus resources for political advocacy, copyright infringement, sexual harassment, and child pornography. Users must adhere to protections provided by software licensing agreements as well as CSU and campus policies regarding intellectual property and state law or policy regarding the use of university names and trademarks.

2. Use of any campus technology resource by any university constituent (faculty, student, staff or general public) to circumvent legitimate copyright protections or illegally access, copy or disseminate copyrighted material is unacceptable and may constitute violation of Federal law and Title 5 of the California Code of Regulations.

F. **Passwords and Credentials**

1. Users who have been authorized to use a password-protected account must follow established procedures for setting, maintaining and changing passwords and may not disclose the password or otherwise make the account available to others without explicit authorization per established procedures.

G. **Authorized Use**

1. Access to campus technology resources is granted to CSUSM faculty, staff and students for purposes related to the campus mission, including but not limited to instruction, research, duties as employees and/or campus-sanctioned activities.
2. Use may also be granted to individuals outside the university if such use is consistent with the mission of the university.
3. An individual may have this privilege revoked if the individual violates the rules set forth in this policy.
4. Access to campus technology resources may be suspended during the course of an investigation, but shall not be revoked without formal review with campus administration.
5. With the exception of implicitly publicly accessible campus technology resources such as websites, permission to use campus technology resources may not be transferred or extended by members of the campus community to individuals or groups who are not associated with the campus without prior approval of an individual designated as having authority to permit use of the information technology resource. Such use must be limited in nature and fall within the scope of the mission of the institution. The authorizing official is expected to ensure that access granted under these circumstances is not abused.
6. Incidental and minimal personal use is permitted provided it does not violate California Government Code Section 8314 or Section 9.1 of this document, does not consume a significant amount of campus technology resources, does not interfere with the individual's or other users' ability to

perform campus-related responsibilities, and otherwise complies with applicable laws, rules, policies, contracts and licenses.

H. **Commercial Activity**

1. Individuals are strictly prohibited from using campus technology resources for unauthorized commercial activities, personal gain or other commercial activities unrelated to campus business. Unauthorized commercial activities includes soliciting, promoting, selling, marketing or advertising products or services, or fundraising for non- CSU-related organizations, non-profit or otherwise.
2. Entities, such as CSU auxiliary organizations, may be authorized by contract to provide commercial services and products to students, faculty and staff, and invited guests of the campus.

I. **Identity Misrepresentation**

1. Users of campus technology resources shall not purposefully misrepresent their identity, either directly or by implication, while communicating electronically. This provision is not intended to limit anonymity, where appropriate, but rather to address purposeful and deliberate use of false identities.

J. **Damage to or Impairment of Campus Technology Resources**

1. Individuals shall not use any campus technology resource in a manner that may cause damage to or impair the campus's technology resources, including but not limited to, any manner that adversely affects the work of others or intentional, reckless or negligent behaviors that might interfere with, disrupt or inflict damage to any computer system, network or related service.
2. Examples include but are not limited to introducing a computer "malware" application, purposefully altering the system or network configuration in such a way as to impact availability, accessing or using any computer, network or electronic data without permission, misusing or allowing misuse, and intentionally inflicting virtual or physical damage to a technology resource. Such behaviors are prohibited on both campus-owned and privately-owned equipment operated on or through campus technology resources.

K. **Access Restrictions**

1. Individuals shall not access, attempt to access, or intentionally enable others to access information or systems to which they have not been granted access. Exploratory activities which extend beyond an individual's assigned computer resources such as port scanning and security scanning are prohibited unless specific authorization has been granted. Unless part of their approved job description, users shall not monitor systems or networks or capture the data residing on or transmitted through campus technology resources.

L. **Reporting of Violations**

1. Effective security is a team effort involving the participation and support of every CSUSM employee, student and affiliate who uses information and/or information systems. Every employee or affiliate who has knowledge or reasonable suspicion of a violation of this policy must follow the applicable procedures for reporting the violation to the proper authorities at their institution.

M. **Compliance**

1. Individuals physically located in other states, countries or jurisdictions are subject to the applicable laws of that jurisdiction in addition to California and federal law when accessing materials electronically through campus technology resources. When electronically accessing material housed in other states or countries through campus technology resources, individuals may also be required to comply with applicable laws of that state or country.

N. **Content**

1. Freedom of thought, inquiry, and expression is a quintessential academic value. Material considered offensive to one person may not be to others and may constitute expression protected by the First Amendment of the United States Constitution. CSUSM relies on the integrity and responsible use of campus technology resources by each of its members and expects adherence to the highest academic standards. Materials that violate applicable laws (e.g., child pornography, copyright infringement, etc.) or CSUSM policy (e.g., sexually explicit content creating a hostile work environment, etc.) may not be accessed through or stored on campus technology resources.

O. **CSUSM Rights and Responsibilities**

1. The campus is committed to protecting users of campus technology resources from illegal or damaging actions by individuals either within or external to the university community. The campus will take steps to help employees, students and affiliates understand the principles described in this acceptable use policy.
2. The campus reserves the right to limit access to technology resources when policies or laws are violated and to use appropriate means to safeguard its technology resources, preserve network/system integrity, and ensure continued service delivery at all times. The campus reserves the right to limit access to campus technology resources when policies or laws are violated and to use appropriate means to safeguard its technology resources, preserve network/system integrity, and ensure continued service delivery at all times. This includes monitoring routing information of communications across its network services and transaction records residing on campus technology resources, scanning systems attached to the campus network for security problems, disconnecting systems that have become a security hazard, and

restricting the material transported across the network or posted on CSUSM system as per the Computer & Network Security Policy[3].

3. Unless otherwise required by law and/or policy, the campus reserves the right to archive and/or remove stored files and messages in order to preserve system integrity. Original electronic materials and/or copies may be retained for specified periods of time on system backups and other locations; however the campus does not warrant that such information can be retrieved.

[1] http://www.calstate.edu/icsuam/sections/8000/8105.0.shtml

[2] Remote wipe capabilities are intended, where possible, to only wipe campus data.

[3] This policy can be found at http://www.csusm.edu/policies/procedure_online.asp?ID=137.

Approval Signatures

Step Description	Approver	Date