I. REFERENCES AND RESOURCES

Federal Policies

U. S. Copyright Law

State Policies

California Penal Code, Section 502

UC Policies

University of California – Policy SVSH Sexual Violence and Sexual Harassment

b. **Integrity of Information Technology resources**: Users shall not interfere with the normal operation of Information Technology resources.

   i. **Modification, damage, or removal of resources**. Users shall not modify, damage, or remove Information Technology resources owned by the University or other users without proper authorization.

   ii. **Encroaching on others' access and use**. Users shall not encroach on others' access and use of the University's Information Technology resources. This includes but is not limited to: the sending of chain-letters or excessive messages; printing excessive copies; excessive use of network capacity; unauthorized modification of data, programs, and configurations; attempting to crash or tie up Information Technology facilities.

   iii. **Unauthorized or destructive programs**. Users shall not intentionally develop or use programs such as, but not limited to viruses, backdoors, logic bombs, Trojan horses, bacteria, and worms that:

      1. Disrupts other users.
      2. Accesses private or restricted portions of the system.
      3. Identifies security vulnerabilities or decrypts secure data
      4. Damages the software or hardware components of an electronic communications resource.

   Notwithstanding the above, the University recognizes the value of research and education in game development, computer security, the investigation of self-replicating code, and other similar pursuits. Such legitimate academic pursuits for research and instruction that are conducted under the supervision of academic personnel are authorized to the extent that the pursuits do not compromise the University's Information Technology facilities.

   iv. **Protecting network integrity**. Users must ensure that proper security is implemented on computers for which they are responsible and that are connected to the network in order to protect the University against attempts to inappropriately access licensed and/or internal data and resources or "hacking" activities. This includes performing reasonable and customary configuration and maintenance (including security updates, patches, etc.), as well as implementing and utilizing adequate access controls (proper passwords, secure protocols, etc.).

   v. **Unauthorized equipment**. Users shall not install or attach any equipment to the UC Merced network without the explicit approval of the Central Information Technology department or a designated delegate.

c. **Unauthorized access**. Users shall not seek or enable unauthorized access.

   i. **Authorization**. Users shall not access Information Technology resources without proper authorization, or intentionally enable others to do so.

   ii. **Password protection**. A user who has been authorized to use a password-protected account shall not disclose the password or otherwise make the account available to others without authorization.

d. **Usage**. Users shall comply with applicable law and University policy.

i. **Hostile working environment or learning environment**. Users shall not use Information Technology resources in a manner that creates a hostile working environment or learning environment (including sexual or other forms of harassment), or that violates obscenity laws.

ii. **Unlawful activities**. Users shall not use Information Technology resources for unlawful activities or activities that violate University policy, including fraudulent, libelous, slanderous, harassing, threatening, or other communications.

iii. **Mass messaging**

)10.2(no)-4.76(ns)-3pamng,, o r otheiesi

officials or their staff from faculty, staff, students, or affiliates expressing personal views may not be written on University letterhead, nor sent in an email from a University computer or electronic email address. Faculty members are encouraged to share their subject matter expertise with elected officials and their staff that is in-line with the University public service mission. Faculty are prohibited from seeking state or federal legislative or budget support for their projects and must state that their verbal or written comments, including those transmitted through electronic mail, do not represent an official position of the University of California. The UC Merced Director of Government Relations will provide guidance and assistance to faculty who are providing subject matter expertise to elected officials or their staff on issues where they are not officially representing the University. Questions related to the expression of political views by faculty, staff, students, or affiliates as individuals through University Information Technology resources should be directed to the UC Merced Director of Government Relations.

ii. **Religious use**. In incidental communications relating to religious activities or issues, the user's University title and/or affiliation may be used only for purposes of identification. A disclaimer (see D.6 above) must be used if such identification might reasonably be construed as implying the support, endorsement, or opposition of the University with regard to any religious activity or issue.

iii. **Commercial use**. The University's Information Technology resources shall not be used for non-University commercial purposes, except as permitted under University policy or with the appropriate approval.

iv. **Advertisements**. The University's Information Technology resources shall not be used to transmit commercial or personal advertisements, solicitations, or promotions, except as permitted under University policy or with the appropriate approval.

V. PROCEDURES

Not Applicable

VI. RESPONSIBILITIES

A.

University's Information Technology services is primarily the responsibility of the Associate Vice Chancellor and Chief Information

agreements. Violators may be referred to their sponsoring advisor, supervisor, manager, dean, vice chancellor, Student Affairs representative, or other appropriate authority for further action.

VII. POLICY OR PROCEDURE REVISION HISTORY

APPENDICES

Not Applicable