Technology Resources Appropriate Use Policy

Effective Date: 06-01-2015
Last Updated: 06-04-2015

Responsible University Officer:
Opinder Bawa
Vice President, Chief Information Officer

Policy Owner:
Director, IT Infrastructure

Policy Contact:
ITS Help Desk

Policy Contents
I. POLICY STATEMENT
II. REASON FOR POLICY
III. SCOPE
IV. AUDIENCE
V. POLICY TEXT
VI. PROCEDURES
VII. RELATED INFORMATION
VIII. DEFINITIONS
IX. FREQUENTLY ASKED QUESTIONS
X. REVISION HISTORY
XI. COMPLIANCE
XII. POLICY EXCEPTION PROCESS
XIII. APPENDICIES
I. POLICY STATEMENT
A. The USF Technology Resources Appropriate Use Policy governs the proper access, use, and management of all USF-owned or -operated technology resources, and the protection of individual users. This policy is administered by the Information Technology Services department (hereinafter referred to as “ITS”) and is to be interpreted in the broadest possible sense. Information contained herein supplements but does not replace applicable laws, regulations, and contracts.

II. REASON FOR POLICY
A. This policy is intended to ensure that USF technology resources are used and managed properly.

III. SCOPE
A. This policy applies to USF technology resources and network usage even in situations where it would not apply to the individual equipment in use. Examples of such usage include, but are not limited to, use of personal computers, servers, email, Internet, WWW, dial-in access, and remote computing. In the event of need for clarification of this policy, such clarification will be determined by ITS.
B. University units that operate their own technology resources may add, with the prior written approval of the unit head and Vice President for Information Technology, individual guidelines that supplement, but do not relax, this policy. In such cases, the unit head must inform his or her users of the supplemental guidelines prior to implementation.
C. Access to technology resources owned or operated by USF imposes certain responsibilities and obligations and is granted subject to USF policies and procedures, contractual obligations, and federal, state, and local laws (hereinafter referred to as “applicable laws”). Applicable University policies and procedures include but are not limited to those contained in the Fogcutter Student Handbook, the General Catalog, the Administrative Staff Handbook, and applicable collective bargaining agreements (all hereinafter referred to as “USF policies and procedures”).

IV. AUDIENCE
A. This policy applies to USF students, faculty, staff, alumni, and others with permission to use USF technology resources.
Technology Resources Appropriate Use Policy
06-01-2015

V. POLICY TEXT

A. Prohibited Activities

1. Technology resources are shared and users must refrain from acts that waste or prevent others from using these resources. Conduct that is contrary to the letter or spirit of this policy, or that adversely affects the University’s mission, is subject to disciplinary action and sanctions as outlined by applicable University policies and procedures as well as applicable laws. Prohibited behavior includes, but is not limited to, the following:

   a. **Academic Dishonesty:** Users may not use computing resources to engage in academic misconduct. Users are expected to act in accordance with the high ethical standards of the University community. Please refer to the Student Academic Integrity Policy in the Fogcutter Student Handbook for more information.

   b. **Denial of Service:** Users may not deliberately attempt to degrade the performance of any computer system or network, or to deprive authorized users or administrators of resources or access to any USF computer system or network.

   c. **Excessive Game Playing:** USF technology resources are not to be used for extensive recreational game playing. Limited recreational game playing may be tolerated within the parameters of each department’s rules. Recreational game players using University computers must give up their seat when others who need to use the facility for academic or research purposes are waiting.

   d. **Harassment:** Users may not violate University policies regarding harassment, discrimination, and other prohibited conduct through use of University-owned or operated technology resources.

   e. **Harmful or Destructive Activities:** Users may not engage in harmful or destructive activities. Such activities include, but are not limited to: creating or propagating viruses, disrupting services, damaging files, intentionally destroying or damaging equipment, software, or data belonging to USF or other users, damaging computer systems, or obtaining unauthorized extra resources. Users may not copy, alter, or destroy anyone else’s personal files, regardless of storage medium, without explicit permission unless authorized or required to do so by law or regulation.
f. **Network Installations:** Users may not, without authorization from ITS, connect any network equipment to the USF campus network. Network equipment includes, but is not limited to: hubs, routers, firewalls, bridges, switches, and modems or any devices that provide network connectivity to more than one individual computer system. Users may not connect to the network any computer that is configured to perform the functions of the aforementioned network equipment.

g. **Permitting Unauthorized Access and/or Anonymous Usage:** Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users. Users may not run network services that allow the anonymous deposit of data on the USF network. For any such data transfer services, security must be provided through usernames and passwords that are traceable to individual users.

h. **Political, Commercial, or Personal Use:** The University is a non-profit, tax-exempt corporation and as such, is subject to applicable laws regarding sources of income, political activities, use of property, and similar matters. It must therefore assure proper use of its resources.

   i. **Political Activity:** Users may not use USF technology resources for partisan political activities where prohibited by applicable laws. Use for political activities not prohibited by applicable laws must have the prior written approval of the Provost or the Vice President for University Life, in consultation with the Office of the General Counsel.

   ii. **Commercial Use:** Users may not use USF technology resources for commercial purposes without the prior written approval of the Vice President for Business and Finance.

   iii. **Personal Use:** Users may not use USF technology resources in connection with compensated outside work or for the benefit of organizations or individuals not related to USF, except in the cases of incidental use, use supporting scholarly pursuits, or other use subject to arrangements between the user and the user’s dean, director, or supervisor. Incidental use for personal business includes occasional communication and other use that has negligible effect on the use of technology resources by others.

   i. **Sharing of Access:** Users may not share passwords and other types of authorization with others. Computer accounts and authorizations are assigned to individual users and users are responsible for any use of their accounts.
j. **Storage of Confidential Data:** Users may not store highly confidential information, as defined by the USF Information Security Policy in unencrypted form on the USF computer, handheld devices, or storage media. Data classified as confidential should also be encrypted. With the exception of certain educational records maintained by adjunct faculty in accordance with FERPA, users may not store confidential or highly confidential data in any form on personally owned computing equipment. Users should refer to the Encryption Policy and the Portable Media Policy.

k. **Unauthorized Access:** Users may not use facilities, accounts, access codes, privileges, or information for which appropriate authorization has not been obtained. Users may not gain unauthorized access to systems through unauthorized use of a special password, loopholes in computer security systems, or another user’s password. Special access to information is to be used only in performance of duties for which access is granted. Information that a user obtains through special access is to be treated as confidential.

l. **Use of Copyrighted Information and Materials:** Users must comply with all applicable laws regarding the use of copyrighted material. Users are responsible for recognizing (i.e. attributing) and honoring the intellectual property rights of others and are prohibited from using, distributing, copying, and storing copyrighted material in violation of University intellectual property policies and copyright laws. Users should refer to the USF Copyright Policy.

m. **Use of Unlicensed Software:** No software may be installed, copied, or used on USF resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all license provisions (e.g. installation, use, copying, number of simultaneous users, terms of license, etc.) must comply with this policy, as well as all applicable laws and contractual agreements.

**B. User Responsibilities**

1. Users are responsible for helping maintain the security and integrity of USF technology resources.

   a. **Security Updates:** Users must keep antivirus definitions and operating system security updates current.

   b. **Backups:** Users are responsible for the security and integrity of USF information stored on personal desktop systems. Users must make regular backups of USF information to a file server, backup tape, CD, DVD, or other storage medium.
c. Access Control: Users are responsible for reasonably controlling the physical and network access to their technology equipment.

d. Protected Content: Users should refer to the Encryption Policy and the Portable Media & External Storage Policy.

e. Awareness of Technology Resources: Members of the University community are responsible for knowing what technology resources, including networks, are available. Information about USF technology resources is available online at myUSF.usfca.edu/its.

C. University Authority

1. The University is responsible for the maintenance and management of USF technology resources.

   a. Control of Access to Information: USF may control access to its information and the devices on which it is stored, manipulated, and transmitted, in accordance with University policies and procedures and applicable laws.

   b. System Administration Access: A System Administrator may access others’ files or accounts for the maintenance of networks and computer and storage systems. Reasons for access include but are not limited to creating backup copies or investigating allegations of misconduct, alleged violations of University policies or procedures, or alleged violations of law.

   c. Monitoring of Usage and Inspection of Files: Units of USF operating technology resources may, without prior notice to the user, routinely monitor and log usage data such as network session connection times and end-points, CPU and disk utilization for each user, security audit trails, and network loading. When necessary, these units may monitor all the activities of and inspect the files of specific users on their computers and networks.

   d. Suspension of Individual Privileges: Units of USF operating technology resources may suspend access privileges of an individual user for reasons relating to the alleged or actual violation of USF policies, contractual obligations, or applicable law.

D. Policy Enforcement

1. Reporting of Misconduct: If a user observes or receives a report of a security or abuse problem, including violations of this policy, with any USF technology resources, the user is encouraged to notify ITS at abuse@usfca.edu. The Information Security Officer will coordinate the incident response.
2. **Investigation and Adjudication of Violations:** Allegations of violations of this policy are resolved in accordance with applicable University policies and procedures. Users found responsible for violating this policy are subject to a full range of sanctions including, but not limited to, the loss of technology resource access privileges, suspension or expulsion from the University, or termination of employment. Some violations may constitute criminal offenses under applicable laws and USF may report such violations to the appropriate authorities.

VI. **PROCEDURES**
A. (None)

VII. **RELATED INFORMATION**
B. USF Copyright Policy, [http://myusf.usfca.edu/system/files/copyright_policy.pdf](http://myusf.usfca.edu/system/files/copyright_policy.pdf)

VIII. **DEFINITIONS**
A. (None)

IX. **FREQUENTLY ASKED QUESTIONS**
A. (None)

X. **REVISION HISTORY**
A. 06-01-2010 – First publication
B. 03-01-2015 – Updated format
C. 06-04-2015 – Added reference to the Fogcutter Student Handbook

XI. **COMPLIANCE**
A. Failure to follow this policy can result in disciplinary action in accordance with the Human Resources Employment Handbook or the Fogcutter Student Handbook and Office of General Counsel employee and labor relations. Disciplinary action for not
following this policy may include termination, as provided in the applicable handbook or employment guide.

XII. POLICY EXCEPTION PROCESS

A. A proposed exception request to ITS Policy requires a formal e-mail explanation related and in support of job function.
B. A proposed exception request to ITS Policy, mentioned in 'XII.A', must be approved via email by respective department or division supervisor, Dean, or VP, before submitted to ITS for review.
C. Forward approved email as stated in 'XII.B' to itshelp@usfca.edu for processing.
D. Evaluation of ITS Policy Exception will escalate internally, and as applicable may include further review by: UITC subcommittee(s), the Information Security Officer, and others as appropriate at the request of VP for IT.

XIII. APPENDICIES

A. (None)