Technology Resources Appropriate Use Policy

Updated and Effective of: 10/1/2016

Responsible University Officer: Vice-President, Chief Information Officer (VP-CIO)

Policy Owner: Associate Vice-President, Information Technology

I. Purpose

The University provides and makes available computing, network, communication, storage, and information technology resources and services to all authorized members of the University community. The technology resources and services collectively known as information assets (e.g. personal computers, printers, servers, databases, email, storage, telephones) are essential to support and deliver the University's mission and run the University's business.

It is University policy that every member of the University community (Users) who access, use, and interact with the information assets does so in an manner that is appropriate, acceptable, legal, and in compliance with University policies, laws, and regulations. This policy protects both the Users and the University.

By implementing this policy the University will:

a. govern the proper access, use, and management of all University owned, operated, and provided information assets,
b. govern the actions of individual Users,
c. reserve the right to audit for compliance to this policy including performing approved monitoring and release of data as necessary or required under law,
d. assure compliance with applicable laws and regulations governing the University's non-profit status,
e. ensure this policy is consistently applied and monitored through the use of a compliance program.

Under this policy Users are responsible for all actions performed under their username and as a consequence usernames and passwords must not be shared. Examples of actions include, but are not limited to, the use of computers and devices, servers, databases, email, network access, Internet web access, and remote access using personally owned devices. Deliberate and inadvertent misuse that causes harm or damage to another person, institution, or entity within or outside of the University, or that violates this and other applicable University policies, Federal, State, or local laws and regulations, is prohibited. Prohibited actions include, but are not limited to, those where Users may:
1. use the information assets to engage in academic misconduct or reduce the standards of honesty and integrity,
2. interfere with the proper functioning of the information assets, deliberately attempt to degrade the performance of any information asset, or deprive access to authorized users and asset administrators,
3. engage in excessive recreational game playing or activities to the detriment of the information assets,
4. use the information assets in breach of University's policies including, but not limited to, those on harassment and discrimination, other prohibited conduct, or to the detriment of the University's reputation,
5. engage in harmful or destructive activities such as propagating malware, hacking, intentional theft, damage, or destruction of information assets,
6. connect unauthorized equipment to the University's network or attempt to circumvent security controls and protocols,
7. permit or facilitate unauthorized access, anonymous use, or placing unapproved data on the University's resources,
8. share access permissions with others or attempt to gain unauthorized access,
9. use the resources and services for partisan political activities unless allowed by law after first obtaining approval from the Office of the General Counsel,
10. use the information assets without prior approval for commercial purposes, or compensated work unrelated to the University, except for limited incidental use,
11. store confidential or highly confidential data on personally owned computing equipment and devices, or in an unencrypted form on University provided equipment or portable storage media,
12. violate use of copyrighted information, intellectual property and materials, and University copyright policies,
13. install or copy software unless permitted by the owner of the software or under the software's terms of use license, contract agreement, or applicable laws, and without ITS approval,
14. export software, technical information, encryption software or technology in violation of US or international export control laws and regulations,
15. fail to keep the standard image and antivirus current on USF owned personal computers, and fail to secure the integrity of the data via regular backups,
16. use the information assets for non-University approved purposes.

II. Scope

This policy applies to all authorized members of the University who have access to and use the information assets, in all locations, both on- and off-campus. More specific policies apply to Users with elevated IT access privileges.
III. Responsibilities

a. The Vice-President, Chief Information Officer (VP-CIO) designates the Associate Vice-President, Information Technology (AVP) to be responsible for the development and maintenance of this policy with consultation from the Office of the General Counsel (OGC).

b. The VP-CIO is responsible for approving and ensuring ongoing compliance with this policy with oversight from the Board of Trustees (BoT) Committee on Information Technology Strategy (CITS).

c. The University Leadership Team are responsible for championing this policy and information security practices in their respective Divisions, Schools, and Colleges, and any substantive revisions as recommended by the VP-CIO.

d. The VP-CIO is responsible for ensuring information assets are secure from unauthorized access (to maintain appropriate confidentiality), unauthorized alterations (to maintain integrity), and available to authorized Users (to maintain availability) enabling the University to meet its mission in an effective and timely manner. The VP-CIO may delegate responsibility for this policy to the AVP.

e. The AVP is responsible for incorporating and maintaining reasonable security processes, practices, procedures, guidelines, and technologies to protect the information assets and enable this policy, and ensuring that this policy is reviewed and updated as necessary.

f. The Information Security Officer (ISO) is responsible for establishing and maintaining an information security program to support this policy, and for coordinating with the AVP on the ITS response to information security incidents, violations, or crimes committed under this policy.

g. All Users, including Third-Parties entrusted with the University's information, are responsible for being familiar with, and complying with, this policy. Users have individual and shared responsibilities to protect the confidentiality, integrity, and availability of the information assets in accordance with University policies, Federal, State, local laws, regulations, and agreements binding the University. Users are required to take information security and awareness training appropriate to their role in support of this policy.

h. Users should understand that the University does not guarantee the privacy of information and should seek further guidance from the AVP if they are unsure of their responsibilities under this policy. The information assets are for University use and must not be used for non-University purposes without prior approval.

i. The OGC will provide legal guidance to this policy.

j. Failure to comply with this policy can result in actions to limit, suspend, or revoke user access to the University's network, email, and other information assets. Members of the University community who knowingly violate this policy may be subject to disciplinary actions that include but are not limited to the policies and procedures contained in the Staff Handbook, the Student Handbook (Fogcutter), applicable Collective Bargaining Agreements, and laws which may include civil and criminal prosecution.
IV. See Related Policies

a. Electronic Communications Policy.
b. Information Security Policy.
c. Technology Acquisition Life Cycle Management Policy