Rule Statement

Rules for responsible computing provide guidance for the appropriate use of System Offices (SO) information resources.

Definitions

Abuse – Excessive or improper use of a resource, intentional destruction, diversion, manipulation, misapplication, or misuse of resources. Also, it is the extravagant or excessive use as to abuse one’s position or authority (System Policy 10.02, Control of Fraud, Waste and Abuse.)

Breach of Security - unauthorized access to information resources or information resources technologies and/or release of password or other confidential information related to computer security.

Custodian of an Information Resource - a person responsible for implementing owner-defined controls and access to an information resource. Custodians may include university employees, vendors and any third party acting as an agent of or otherwise on behalf of the university and/or the owner.

Fraud – any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain. (A willful or deliberate act or failure to act with the intention of obtaining an unauthorized benefit, such as money or property, by deception or other unethical means.) For purposes of this rule, fraud and fraudulent activities include, but are not limited to, such things as:

- Theft of any system asset including money, tangible property, time, trade secrets and intellectual property
- Embezzlement
- Bribery/rebate/kick-back
- Misappropriation, misapplication, destruction, removal or concealment of university property
- Forgery, alteration or falsification of documents
- Conflicts of interests
Harmful Access - creating a computer malfunction or interruption of operation; alteration, damage, or destruction of data; or, injection of malicious software.

Information Resources - the procedures, computer equipment, computing facilities, software and data which are purchased, designed, built, operated and maintained to collect, record, process, store, retrieve, display, report and transmit information.

Owner of an Information Resource (owner) - a person responsible for a business function and for determining controls and access to information resources supporting that business function.

Waste - intentional or unintentional, thoughtless or careless expenditure, consumption, mismanagement, use or squandering of resources to the detriment of the organization. Waste also includes incurring unnecessary costs as a result of inefficient or ineffective practices, systems or controls.

Official Rule/ Responsibilities/ Process

1. GENERAL

1.1 System Offices recognizes the importance of information technology to students, faculty, and staff in scholarly pursuits, professional development, service activities, personal development, and everyday work.

1.2 Use of these resources and facilities is a privilege and requires that individual users act in compliance with SO Rules. The SO provides users with an account that permits use of the computing resources and facilities within guidelines established by SO. Users must respect the integrity of computing resources and facilities, respect the rights of other users, and comply with applicable laws (local, state, federal and international), System Policies, System Regulations, SO Rules and contractual agreements. The SO reserves the rights to limit, restrict, or deny computing privileges and access to its information resources for those who violate, or who are under investigation for allegedly violating, local, state, federal and international laws, System Policies, System Regulations, SO Rules, or contractual agreements.

2. PRIVACY

While there is no expectation of privacy beyond that which is specified in applicable privacy laws, the privacy of data will be maintained in the course of all custodial operations and access. Personnel (non-owner) will not access data beyond that which is needed to maintain efficient and secure operations of the systems. Contents of electronic files will be examined or disclosed only when authorized by their owners, approved by an appropriate System Offices official, or required by law (see System Offices SAP 29.01.99.S1.17).
3. COPYRIGHT LAWS

Copyright laws apply to the electronic environment. Users should assume that works communicated through a network are subject to copyright unless specifically stated otherwise. Utilization of any electronically transmitted information should be within the "fair use" principle unless permission of the copyright author is obtained.

4. CRIMINAL AND ILLEGAL ACTS

Computing resources of the SO, which include the hardware, software, and network environment, shall not be used for illegal activities. Any such use of these resources will be dealt with by the appropriate SO authorities and/or other legal and law enforcement agencies. Criminal and illegal use may involve unauthorized access, intentional corruption or misuse of information resources or facilities, theft, obscenity, child pornography, illegal discrimination, sexual harassment and related retaliation.

5. AUTHORIZED USE

Computing resources are provided by the SO to accomplish tasks related to the SO mission. Computing resources may not be used for commercial activities or illegal activities. Incidental personal use of computing resources by employees is governed by System Policy 33.04, Use of System Resources.

6. INDIVIDUAL RESPONSIBILITY FOR USE OF COMPUTING RESOURCES

It is expected that all members of the SO community will use these resources and facilities in accordance with System policies, regulations and SO rules. Failure to fulfill these responsibilities may lead to the cancellation of computer account(s), disciplinary action by the SO, and/or referral to legal and law enforcement agencies. In addition to complying with the other provisions of this rule, individuals using the SO computing resources or facilities are required to:

   a. Use communal resources with respect for others. Disruptive mailings and print jobs, tying up work stations, and other disproportionate uses of computing facilities prevent others from using these resources.

   b. Protect passwords and use of accounts. Individuals are not permitted to use accounts or passwords for which they are not the designated user. Confidential information contained on various computers should not be shared with others except when that person is authorized to know such information.

   c. Secure confidential information contained on various information resources and not provide access to any individual who is not authorized to access such information.
d. Report improper use of information resources and facilities. Improper use of information resources and facilities may include:

1. breach of security
2. harmful access; or
3. any other unauthorized access or use.

e. Comply with the request of an information resource owner or custodian (e.g., system administrator) regarding use of that resource.

f. Report fraud, waste, or abuse using System Offices information resources and facilities in accordance with System Policy 10.02.

g. Report any incidents of illegal discrimination, sexual harassment and related retaliation using SO information resources and facilities according to System Regulation 08.01.01, Civil Rights Compliance.

h. Respect the forum (including Listserv, social media, public computing facilities) when communicating ideas to others via SO information resources technologies, email accounts and any other university information resource (including access to the Internet). All communications should reflect high ethical standards and mutual respect and civility.

Related Statutes, Policies, or Requirements

Supplements System Policy 29.01, System Policy 33.04, System Policy 21.04, and System Policy 07.01

Contact Office

Office of the System Chief Information Officer