Acceptable Use of Information Technology Resources

Effective: November 8, 2012
Contact: Office of the Chief Information Officer (CIO)

Contents

Introduction

Iowa State University's Acceptable Use of Information Technology Resources policy (AUP) provides for access to information technology (IT) resources and communications networks within a culture of openness, trust, and integrity. In addition, Iowa State University is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

1. Purpose

The purpose of this policy is to outline the ethical and acceptable use of information systems at Iowa State University. These rules are in place to protect students, faculty, and staff; i.e., to ensure that members of the Iowa State University community have access to reliable, robust IT resources that are safe from unauthorized or malicious use.

Insecure practices and malicious acts expose Iowa State University and individual students, faculty, and staff to risks including virus attacks, compromise of network systems and services, and loss of data or confidential information. Security breaches could result in legal action for individuals or the university. In addition, security breaches damage the university's reputation and could result in loss of services. Other misuses, such as excessive use by an individual, can substantially diminish resources available for other users.

top

2. Scope

The AUP is an integral part of IT security policies and applies to faculty, staff, and students as well as any other individuals or entities who use information and IT resources at Iowa State University. This policy applies to all IT resources owned or leased by Iowa State University and to any privately owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, storage media, the campus network, and the Internet.

Securing and protecting these significant and costly resources from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the Iowa State University community who accesses and uses IT resources. Therefore, every user of Iowa State University's IT resources is required to know the policies and to conduct their activities within the scope of the AUP, the Iowa State University **Information Technology Security policy**, and the **Policies, Standards, and Guidelines for IT Security** (see Resources below). Failure to comply with this policy may result in loss of computing privileges and/or disciplinary action.

3. Policy Statement

Unless otherwise specified in this policy or other university policies, use of university information technology resources is restricted to purposes related to the university's mission. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, official business with the university, and other university-sanctioned activities. Individuals may not share with or transfer to others their university accounts including network IDs, passwords, or other access codes that allow them to gain access to university information technology resources.

Colleges, departments, and other administrative units have considerable latitude in developing complementary technology use policies and procedures, as long as they are consistent with this policy and any other applicable technology use policies of the university.

Incidental personal use of information technology resources must adhere to all applicable university policies. Refer to **Personal Use and Misuse of University Property policy** (see Resources below). Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's university responsibilities, or adversely impact or conflict with activities supporting the mission of the university.

top

4. Unacceptable Use

Users are prohibited from engaging in any activity that is illegal under local, state, federal, or international law or in violation of university policy. The categories and lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.1. Excessive Non-Priority Use of Computing Resources

Priority for the use of IT resources is given to activities related to the university's missions of teaching, learning, research, and outreach. University computer and network resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of IT resources, such as recreational activities and non-academic, non-business services.

4.2. Unacceptable System and Network Activities

Unacceptable system and network activities include:

4.2.1. Engaging in or effecting security breaches or malicious use of network communication including, but not limited to:

4.2.1.1. Obtaining configuration information about a network or system for which the user does not have administrative responsibility.

4.2.1.2. Engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network.

4.2.1.3. Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.

4.2.1.4. Interfering with or denying service to another user on the campus network or using university facilities or networks to interfere with or deny service to persons outside the university.

top

4.3. Unauthorized Use of Intellectual Property

Users may not use university facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

4.3.1. Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.

4.3.2. Using, displaying, or publishing licensed trademarks, including Iowa State University's trademarks, without license or authorization or using them in a manner inconsistent with the terms of authorization.

4.3.3. Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.

4.3.4. Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.

4.3.5. Using computing facilities and networks to engage in academic dishonesty prohibited by university policy (such as unauthorized sharing of academic work or plagiarism).

4.4. Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

4.4.1. Setting up file sharing in which protected intellectual property is illegally shared.

4.4.2. Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

4.4.3. Inappropriate use or sharing of university-authorized IT privileges or resources.

4.4.4. Changing another user's password, access, or authorizations.

4.4.5. Using an Iowa State University computing asset to actively engage in displaying, procuring, or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.

4.4.6. Using an Iowa State University computing asset for any private purpose or for personal gain.

top

4.5. Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of the university and to individual communication among faculty, staff, students, and their correspondents. Individuals are required to know and comply with the university's policy on **Mass Email and Effective Electronic Communication** (see Resources below).

Key **prohibitions** include:

4.5.1. Sending unsolicited messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material, except as approved under the policy on Mass Email and Effective Electronic Communication.

4.5.2. Engaging in harassment via electronic communications whether through language, frequency, or size of messages.

4.5.3. Masquerading as someone else by using their email or internet address or electronic signature.

4.5.4. Soliciting email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.5.5. Creating or forwarding "chain letters" or solicitations for business schemes.

4.5.6. Using email originating from Iowa State University provided accounts for commercial use or personal gain.

4.5.7. Broadcasting e-mail from a university account to solicit support for a candidate or ballot measure, or otherwise using e-mail systems in a concerted effort to support a candidate or ballot measure.

5. Enforcement

The Acceptable Use of Information Technology Resources policy is enforced through the following mechanisms.

5.1. Interim Measures

The university may temporarily disable service to an individual or a computing device, when an apparent misuse of university computing facilities or networks has occurred, and the misuse:

5.1.1. Is a claim under the Digital Millennium Copyright Act (DMCA)

5.1.2. Is a violation of criminal law

5.1.3. Has the potential to cause significant damage to or interference with university facilities or services

5.1.4. May cause significant damage to another person

5.1.5. May result in liability to the university

An attempt will be made to contact the person responsible for the account or equipment prior to disabling service unless law enforcement authorities forbid it or Information Technology Services staff determine that immediate action is necessary to preserve the integrity of the university network. In any case, the user shall be informed as soon as possible so that they may present reasons in writing why their use is not a violation or that they have authorization for the use.
top

5.2. Suspension of Services and Other Action

Users may be issued warnings, may be required to agree to conditions of continued service, or may have their privileges suspended or denied if:

5.2.1. After hearing the user's explanation of the alleged violation, an IT provider has made a determination that the user has engaged in a violation of this code, or

5.2.2. A student or employee disciplinary body has determined that the user has engaged in a violation of the code.

5.3. Disciplinary Action

Violations of the Iowa State University Acceptable Use of Information Technology Resources policy may be referred for disciplinary action as outlined in the Student Disciplinary Regulations and applicable faculty and staff handbooks or collective bargaining agreement. The university may assess a charge to offset the cost of the incident.

top

Resources

Links

- Information Technology Security policy
- Electronic Privacy policy
- Personal Use and Misuse of University Property policy
- Mass Email and Effective Electronic Communication policy
- Student Disciplinary Regulations (Code of Conduct)