Policy Contents

Policy Information

Effective Date:
May 7, 2019
Last Revised Date:
December, 2021
Policy Number:
ISO-700
Responsible Unit:
Information Security Office
Email:
security@arizona.edu [1]

Purpose and Summary

This document establishes the Acceptable Use of Computers and Networks Policy for the University of Arizona. This policy promotes the secure, ethical, and lawful use of the University Information Resources.

Each User of the University Information Systems (including subsystems) as well as other workstations, devices, network infrastructure, and other information technology owned or operated by or on behalf of the University is responsible for their activity. This policy establishes requirements for the acceptable use of such resources.

Scope

This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of the University. All University-Related Persons with access to University Information or computers and systems operated or maintained on behalf of the University are responsible for adhering to this policy.

Definitions

CISO: The senior-level University employee with the title of Chief Information Security Officer.

Information Resources: University Information and related resources, such as equipment, devices, software, and other information technology.

Information System: A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

ISO: The University Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

System Administrator: A User with a level of access above that of a normal User, or with supervisory responsibility for Information Systems and Information Resources. Examples of System Administrators include, but are not limited to, a Database Administrator, a Network Administrator, a Central Administrator, a superuser, or any other privileged User.

Unit: A college, department, school, program, research center, business service center, or other operating Unit of the University.

University Information: Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.

University-Related Persons: University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University, and third-party contractors engaged by the University and their agents and employees.

User: Individual or group that interacts with a system or benefits from a system during its utilization.

Policy

A. All Classifications of University Information

1. Each User must:
    a. **Take no actions that violate the University Code of Conduct, Code of Academic Integrity, Human Resources policies, Information Security Policies, or other applicable law, regulation, Arizona Board of Regents (“ABOR”) policy, or University policy.**
        i. As with other conduct as a University-Related Person, a User’s use of Information Resources is subject to all applicable law and University policies. In the event of a conflict between policies or other legal obligations, the obligation imposing the more restrictive use shall govern.
        ii. Using University computer or network resources in violation of policy or for illegal

activity is strictly prohibited. Prohibited uses may include, but are not limited to, harassment and intimidation of individuals in violation of the University Nondiscrimination and Anti-Harassment Policy [2], obscenity, child pornography, threats, or theft. Examples of misuse also include attempting to gain unauthorized access to data, attempting to breach security measures on any electronic communications software or system, attempting to intercept electronic communication transmissions without proper authority, and violating intellectual property or defamation laws. Do not use computer or network resources to send, post, or display slanderous or defamatory messages, text, graphics, or images.

iii. Each User accepts the responsibility to become informed about and to comply with all applicable laws and policies.

b. **Follow established security controls that protect information, data, and systems.**
   i. Examples of such security controls include, but are not limited to, handling University Information in accordance with requirements documented in the University Information Handling Standard [3] and ensuring that default passwords are changed using strong password methodologies, as defined in the University Password Standard [4].
   ii. Examples of failure to follow such security measures include, but are not limited to, using a computer account or password that a User is not authorized to use, using the campus network to exceed authorized access to a University computer system or any other computer system, and using network protocol analyzers or other tools to attempt to breach the confidentiality of data or passwords.
c. **Clearly and accurately identify oneself in electronic communications.**
   i. Examples of violations include forging or misrepresenting one's identity, or altering or concealing the source of electronic communications, such as creating or editing an email to make it appear as if the message was sent by someone else.
d. **Use computer and network resources efficiently.**
   i. Users may use University computer and network resources for incidental personal purposes, provided that such use does not unreasonably interfere with the use of computing and network resources by other Users, or with the University operation of computing and network resources, interfere with the User's employment or other obligations to the University, or violate this policy or other applicable policy or law. Examples of inappropriate use include sending unsolicited email to large numbers of people to promote products or services, and engaging in unauthorized peer-to-peer file sharing.
   ii. The University retains the right to set priorities on use of its computer and network resources and to limit recreational or personal uses when such uses could reasonably be expected to cause strain, directly or indirectly, on any computing facilities; to interfere with research, instructional, or administrative computing requirements; or to violate applicable policies or laws.
e. **Ensure that the use of computer resources and networks is oriented toward the academic and other missions of the University.**
   i. Use of the User's computer account or the network for profit or commercial gain, except as permitted under applicable University policies, is prohibited. Examples include use of a University computer account to engage in consulting services, software development for private profit, advertising products/services, crypto-currency mining, and/or other commercial profit-based endeavors.
f. **Respect copyright and intellectual property rights.**
   i. Users must adhere to copyright laws, the University Intellectual Property Policy [5], and the terms and conditions of any applicable agreements (whether for software licensing, database licensing, or otherwise) entered into by the

University. Any form of original expression fixed in a tangible medium is subject to copyright, even if there is no copyright notice. Examples include music, movies, graphics, text, photographs, artwork, and software, distributed in any medium, including online. The use of a copyrighted work (such as copying, downloading, file sharing, distribution, public performance, etc.) requires either the copyright owner's permission, or an exemption under the Copyright Act. The law also makes it unlawful to circumvent technological measures used by copyright owners to protect their works.

g. **Respect the integrity of the University computing and network resources.**
    i. Misuse of University computing and network resources includes, but is not limited to, stealing or damaging equipment or software, attempting to circumvent installed data protection methods that are designed and constructed to provide secure data and information, attempting to interfere with the physical computer network or related hardware, or attempting to degrade the performance or integrity of any campus network or computer system.
h. **Respect individual privacy and confidentiality.**
    i. Those who have access to personal information stored on or transmitted through University computing and network resources must respect individual privacy and confidentiality, consistent with applicable laws and University policies regarding the collection, use, and disclosure of personal information. All use of any such information must comply with the University Privacy Statement [6] and other applicable Unit Privacy Notices issued pursuant to the University Electronic Privacy Policy [7].
    ii. Users should consult the University Privacy Statement [6] for information on how their personal information may be handled by the University.
    iii. Users with access to University Information beyond what is generally available (e.g., system, network, and database administrators, among others) may only use such access in a way consistent with applicable laws, University policies, and accepted standards of professional conduct, including as set forth in the Acceptable Use for System Administrators Policy [8].
i. **Respect and adhere to other departmental/college/Internet Service Provider's acceptable use policies.**
    i. When using a University computer system or network to connect to a non-University system or network, Users must adhere to the prevailing policies governing that system or network. However, this does not in any way reduce or release the obligation to abide by this and other policies governing the use of University computer systems and networks.
j. **Allow System Administrators or other authorized individuals to perform routine maintenance and operations, security reviews, and respond to emergency scenarios.**

2. Each University-Related Person who accesses the University Information Resources through a University-provided NetID is required to read and acknowledge a summary of this Policy and related requirements both as a condition of obtaining a NetID and again annually, at minimum. Additionally, a summary of this Policy and related requirements is required to be displayed to, and agreed to by, Users prior to accessing University Information Resources when no NetID login is required.

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

The ISO must develop, test, review, maintain, and communicate a representation of the University-wide information security posture to University leadership. The ISO is authorized to initiate mechanisms to track the effective implementation of information security controls associated with this policy and to produce reports measuring individual or Unit compliance to support University decision making.

Recourse for Noncompliance

The ISO is authorized to limit network access for individuals or Units not in compliance with all information security policies and related procedures. In cases where University resources are actively threatened, the CISO must act in the best interest of the University by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the CISO is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, the University may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

In addition, violations of this Policy are subject to sanctions prescribed in other ABOR and University Policies, including, but not limited to, the following policies: ABOR Code of Conduct, Student Code of Conduct, Code of Academic Integrity, Classified Staff Human Resources Policy Manual, and University Handbook for Appointed Personnel.

Exceptions

Requests for exceptions to any information security policies may be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the CISO for review and approval pursuant to the exception procedures published by the CISO [9].

Frequency of Policy Review

The CISO must review information security policies and procedures annually, at minimum. This policy is subject to revision based upon findings of these reviews.

Responsibilities

University-Related Persons

All University-Related Persons are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.

Information Owners and Information System Owners

Information Owners and Information System Owners are responsible for implementing processes and procedures designed to provide assurance of compliance with the minimum standards, as defined by the ISO, and for enabling and participating in validation efforts, as appropriate.

Chief Information Security Officer

The ISO must, at the direction of the CISO:

- identify solutions that enable consistency in compliance and aggregate and report on available compliance metrics;
- develop, establish, maintain, and enforce information security policy and relevant standards and processes;
- provide oversight of information security governance processes;
- educate the University community about individual and organizational information security responsibilities;
- measure and report on the effectiveness of University information security efforts; and
- delegate individual responsibilities and authorities specified in this policy or associated standards and procedures, as necessary.

Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers

All Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers must take appropriate actions to comply with information technology and security policies. These individuals have ultimate responsibility for University resources, for the support and implementation of this policy within their respective Units, and, when requested, for reporting on policy compliance to the ISO. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Related Information*

- Intellectual Property Policy [5]
- ISO Website [10]
- University Password Standard [11]
- University Information Handling Standard [12]
- University Handbook for Appointed Personnel [13]
- Classified Staff Human Resources Policy Manual [14]
- Student Code of Conduct [15]
- Misuse of University Assets [16]
- Approved Use of University Computing and Communications Equipment [17]
- Electronic Privacy Policy [7]
- Electronic Privacy Statement [18]
- Family Educational Rights and Privacy Act (FERPA) Compliance [19]
- Official Student E-mail Policy [20]
- Use of E-mail for Official Correspondence with Employees [21]
- U.S. Copyright Office [22]
- Copyright and Fair Use [23]
- University Libraries Copyright Guide [24]
- Off Campus Use and Location Policy [25]

Revision History*

02/01/2023: In the Policy Section, under paragraph A.1.b.i. - revised link names and under paragraph A.1.d.i. - made format changes. Non-substantive revisions.

12/2021: System Administrator defined term added; substantive revisions to Policy Section A - All Classifications of University Information; revision to Tracking, Measuring and Reporting and addition of Information Owners and Information System Owners responsibilities under the Compliance and Responsibilities Section; Related Information Section updated; several hyperlinks

updated.

01/24/2020: Non-substantive updates.

03/19/2019: Replaces Interim policy.

Source
URL:https://policy.arizona.edu/information-technology/acceptable-use-computers-and-networks-policy

Links
[1] mailto:security@arizona.edu [2] https://policy.arizona.edu/human-resources/nondiscrimination-and-anti-harassment-policy [3] http://confluence.arizona.edu/login.action?os_destination=%2Fpages%2Fviewpage.action%3FspaceKey%3DUAIS%26title%3DISO-400-S2%2BInformation%2BHandling%2BStandard&permissionViolation=true [4] https://confluence.arizona.edu/display/UAIS/ISO-800-S1+Password+Standard [5] https://policy.arizona.edu/research/intellectual-property-policy [6] https://privacy.arizona.edu/privacy-statement [7] https://policy.arizona.edu/information-technology/electronic-privacy-policy [8] https://policy.arizona.edu/information-technology/acceptable-use-system-administrators-policy [9] https://confluence.arizona.edu/pages/viewpage.action?spaceKey=UAIS&title=ISO-100-P1+Information+Security+Office+Policy+Exception+Request+Procedure [10] https://security.arizona.edu/content/policy-and-guidance [11] http://confluence.arizona.edu/pages/viewpage.action?spaceKey=UAIS&title=ISO-800-S1+Password+Standard [12] http://confluence.arizona.edu/pages/viewpage.action?spaceKey=UAIS&title=ISO-400-S2+Information+Handling+Standard [13] http://policy.arizona.edu/university-handbook-appointed-personnel [14] http://policy.arizona.edu/classified-staff-human-resources-policy-manual [15] https://public.azregents.edu/Policy%20Manual/5-308-Student%20Code%20of%20Conduct.pdf [16] http://policy.arizona.edu/business-and-finance/misuse-university-assets [17] http://policy.arizona.edu/information-technology/approved-use-university-computing-and-communication-equipment [18] https://security.arizona.edu/content/privacy-statement [19] http://www.registrar.arizona.edu/personal-information/family-educational-rights-and-privacy-act-1974-ferpa [20] http://policy.arizona.edu/information-technology/official-student-e-mail-policy-use-e-mail-official-correspondence-students [21] http://policy.arizona.edu/information-technology/use-e-mail-official-correspondence-employees [22] http://www.copyright.gov/ [23] http://fairuse.stanford.edu/ [24] http://new.library.arizona.edu/research/copyright [25] https://policy.fso.arizona.edu/pmm/1100/1130