Policy Contents

Policy Information

Effective Date:
May 27, 2008
Last Revised Date:
April, 2017
Policy Number:
IS-100
Responsible Unit:
UA Information Security
Phone:
(520) 621-8476
Email:
infosec@email.arizona.edu [1]

Purpose and Summary

University resources, information, and technology have become increasingly important to faculty, staff, and students for academic and administrative purposes. At the same time, internal and external threats to the confidentiality, integrity, and availability of these resources have increased. Security breaches are commonplace and universities continue to be popular targets for attack. Critical University resources—such as research, patient care, business transaction, student, and employee nonpublic personal data—must be protected from intrusion and inappropriate use or disclosure. Devices must be set up and routinely maintained and updated so that they prevent intrusion and other malicious activities.

The purpose of this policy is to ensure that all individuals within its scope understand their responsibility in reducing the risk of compromise and take appropriate security measures to protect University resources. Access to University resources is a privilege, not a right, and implies user responsibilities. Such access is subject to Arizona Board of Regents and University policies,

standards, guidelines, and procedures, and federal and state laws.

This policy is especially focused on protecting critical University resources and is intended to require those responsible to safeguard University resources in an appropriate manner.

Scope

This policy and all implementing standards and procedures apply to individuals using, accessing, storing, transmitting, or overseeing University resources, directly or by means of a personally acquired device, including but not limited to

- Vice presidents, deans, directors, department heads, and heads of centers
- Research project principal investigators and their collaborators
- Affiliates, associates, and volunteers
- Faculty, staff, and students
- Third-party vendors, including cases where vendor-owned and/or -managed equipment is housed or used in units

Definitions

Affiliates: Select individuals from institutions, hospitals, and clinics who have been afforded contractual affiliate status by the Office of the Provost. Affiliates do not receive a salary from the University for the duties and services they perform.

Associates: Individuals such as unpaid faculty, principal investigators, visiting scholars, dissertation special members, and others who are regularly engaged in activities that directly support the teaching and research mission of the University but who are not compensated by the University through salary.

Attack: An attempt to gain unauthorized access or deny authorized access to a U*niversity resource*.

Availability: The degree to which information and vital services are accessible for use when required.

Compromise: An unauthorized intrusion into a University resource where unauthorized disclosure, modification. or destruction of confidential University data may have occurred.

Confidentiality: the degree to which confidential University data are protected from unauthorized disclosure.

Device: Any apparatus used to access, store, transmit, or interface with a University resource. This includes but is not limited to computers (servers, workstations, and laptops), PDAs, printers, network appliances, devices situated behind firewalls, Network Address Translation devices, or use of Virtual Private Networks.

Incident: An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information technology operation; or violation of explicit or implied acceptable usage policy (including the Acceptable Use of Computers and Networks policy). The Incident Response Standard provides several examples of incidents.

Integrity: The degree to which the accuracy and completeness of information and computer

software are safeguarded to protect the business process for the University.

Security Breach: An unauthorized intrusion into a University resource where unauthorized disclosure, modification, or destruction of confidential University data may have occurred.

Unit: Any University college, department, school, program, research center, business service center, or other operating unit.

University Resource: Data in any form and recorded in any manner, and computer-related resources operated, owned, or leased by the University, including but not limited to

- Networks and network appliances
- Computers (servers, workstations, and laptops)
- Printers
- Software and applications
- Thumbdrives, paper, etc.
- Any other computer-related equipment, device, or hardware used to access, store, transmit, or interface with another University resource

Volunteer: An individual, such as a docent, 4-H worker, event coordinator, or other person, who does not meet the criteria for affiliate or associate appointments and is not a University employee. Volunteers perform services for the University without coercion or expectation of compensation, benefits, or future employment.

Vulnerability Assessment: An audit by a responsible party that is intended to identify potential vulnerabilities in a computer system or network.

Policy

Each unit will protect University resources by adopting and implementing, at a minimum, the security standards and procedures developed by the Chief Information Security Officer (CISO). All units must meet the minimum standards. Units are encouraged to adopt standards that exceed the minimum requirements for the protection of University resources.

Individuals within the scope of this policy are responsible for complying with this policy and the unit’s policy, if one exists, to ensure the security of University resources.

Recourse for Noncompliance

In cases where University resources are actively threatened, the CISO will act in the best interest of the University by securing the resources. When possible, the CISO will abide by the incident handling procedures to mitigate the threat. In an urgent situation requiring immediate action and leaving no time for collaboration, the CISO is authorized to disconnect any affected device from the network. University resources are subject to "vulnerability assessment" and safeguard verification by the CISO.

Individuals who are subject to but do not comply with this policy and mandatory implementation of standards will be subject to remedial action in accordance with Arizona Board of Regents and University policies and procedures (including but not limited to the Arizona Board of Regents Code of Conduct, Student Code of Conduct, Code of Academic Integrity, Classified Staff Human Resources Policy Manual, University Handbook for Appointed Personnel, and the policy on the Acceptable Use of Computers and Networks) or contract terms, as appropriate. Violations of this policy may result

in loss of data access privileges, administrative sanctions, and personal civil and criminal liability.

Exceptions

The CISO may grant exceptions to this policy and/or standards after preliminary review.

Support

All incidents of actual or suspected compromise must be reported immediately to the CISO.

For assistance in resolving compromises or vulnerabilities, computer users should contact their local system administrator, network manager, University Information Technology Services, and/or the CISO.

System administrators or network managers should refer to the standard on incident response for technical assistance in investigating the incident.

Compliance and Responsibilities

Vice Presidents, Deans, Directors, Department Heads, and **Heads of Centers:** Pursuant to the President's memorandum of February 21, 2007, all Vice Presidents, Deans, Directors, and Department Heads have the management authority and are expected to take appropriate actions to comply with information technology and security policies. These individuals have ultimate responsibility for University resources and implementation of this policy within their respective units. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers must designate an Information Security Liaison to serve as the primary contact between the respective unit and the Office of Information Security for all matters relating to information security.

The **Vice President, Information Strategy and University Libraries (VPISUL)** and the **Chief Information Security Officer (CISO)** are responsible for establishing and enforcing information security policy and supporting standards and procedures.

The CISO in consultation with the VPISUL will have primary responsibility for

- Oversight of information security
- Development, revision, and oversight of security policy, standards, and procedures.
- Implementation and enforcement of this policy
- Educating the University community about security responsibilities

The CISO will issue policies, standards, procedures, and additional guidance to assist units in implementing this and other information security-related policies. This policy is the governing foundation for future policies, standards, and procedures related to information security.

The CISO may delegate individual responsibilities and authorities specified in this policy or associated standards and procedures.

Related Information*

Acceptable Use of Computers and Networks [2]

Incident Response Standard [3]

Revision History*

Title updates April 10, 2017

Links
[1] mailto:infosec@email.arizona.edu
[2] http://policy.arizona.edu/information-technology/acceptable-use-computers-and-networks
[3] http://security.arizona.edu/sites/securitysiab/files/is-s1100.pdf