

## **I. Introduction**

*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.

All italicized terms used in this policy are defined in the Information Security Terms Guideline.

## **II. Authority**

The Chief Information Officer (CIO) and the University Information Security Officer (UIISO) are responsible for establishing and enforcing information security policy and supporting standards and procedures. 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.

## **III. 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*.

#### **IV. Responsibilities**

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.

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

The UIISO in consultation with the CIO 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 UIISO 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 UIISO may delegate individual responsibilities and authorities specified in this policy or associated standards and procedures.

Vice Presidents, Deans, Directors, Department Heads or 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.

#### **V. Policy Statement**

Each *unit* will protect *university resources* by adopting and implementing, at a minimum, the security standards and procedures developed by the *UIISO*. 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*.

## **VI. Recourse for Non-Compliance**

In cases where *university resources* are actively threatened, the UISO will act in the best interest of the university by securing the resources. When possible, the UISO 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 UISO is authorized to disconnect any affected device from the network. *University resources* are subject to *vulnerability assessment* and safeguard verification by the UISO.

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 Personnel 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.

## **VII. Exceptions**

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

## **VIII. Support**

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

For assistance in resolving *compromises* or vulnerabilities, computer users should contact their local system administrator, network manager, UITS and/or the UISO.

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

## **IX. Related Guidance**

Information Security Terms Guideline (IS-G100)  
Standards, Procedures and Guidelines at <http://security.arizona.edu>

## **Revision History**

Initial Draft	5/25/06
Effective Date	/ /08