

	Administrative Policy Statement
	Category – Information Management and Technology
IT Resource User Responsibilities	

Effective: January 1, 2007
Responsible Office: Office of Information Security
Vice President: Vice President for Administration
Approved:


President

Brief Description: Establishes *IT security* requirements for all *IT resource users* in protecting University information and *IT resources*.

I. INTRODUCTION

This policy establishes the Information Technology (*IT*) *security* safeguards that must be taken by every person using a University *IT resource* or otherwise accessing University information. Additional safeguards may be appropriate, depending on the situation and its inherent risk to University information and *IT resources*.

This policy does not impose restrictions that are contrary to the University's established culture of sharing, openness, and trust. However, the University is committed to implementing the safeguards necessary to ensure the privacy of personal information, the availability of University information and *IT resources*, and the integrity of University operations.

II. POLICY STATEMENTS

- A. It is the responsibility of every *IT resource user* to know the University's *IT security* requirements and to conduct her/his activities accordingly. *IT resource users* shall comply with the following requirements:
- 1. Protect the Privacy of Others.** Users shall respect the privacy of others when handling personal information and shall take appropriate precautions to protect that information from unauthorized disclosure or use.
 - 2. Do Not Store Sensitive Information on Workstations and Mobile Devices, Except When Specifically Needed for Business Purposes.** Ordinarily, *sensitive information* shall not be stored on workstations and mobile computing devices (laptops, flash drives, backup disks, etc.) unless specifically justified for business purposes and appropriately secured. If *sensitive information* is stored on a workstation or mobile computing device or transmitted to an external network or organization, *IT resource users* shall encrypt or adequately protect that information from disclosure. In addition to encryption, other protections may include the use of passwords, automatic logoffs, and secure Internet transmissions. The protection of *sensitive information* shall be in accordance with campus *IT security* requirements and other guidance as available from the appropriate IT service center or help desk.

3. **Keep a Clear Desk and Clear Computer Screen.** *IT resource users* shall keep all *sensitive information* out of plain sight unless in use and shall not leave such information displayed when it is not needed.
4. **Protect Workstations and Other Computing Devices.** *IT resource users* are responsible for helping to maintain the security of workstations and other computing devices by striving to protect them from unauthorized access and malicious software infections (e.g., viruses, worms, and spyware). Users shall consult the appropriate IT service center or help desk for guidance on protecting their computing devices.
5. **Protect Passwords, Identification Cards, and Other Access Devices.** Passwords, identification cards, and other access devices are used to authenticate the identity of individuals and gain access to University resources. Each person is responsible for protecting the access devices assigned to her or him and shall not share the devices with others. If an access device is compromised, lost, or stolen, the individual shall report this to the appropriate IT service center or help desk as soon as possible so that the access device is not used by an unauthorized person.
6. **Report Security Violations, Malfunctions, and Weaknesses.** *IT resource users* shall report security related events; known or suspected violations of *IT security* policy; and inappropriate, unethical, and illegal activities involving University *IT resources*. Users shall follow the reporting process applicable to their campus. If unsure of the local incident reporting process, users shall call the appropriate IT service center or help desk.
7. **Utilize University Information and IT Resources for Authorized Purposes Only.** *IT resource users* shall access or otherwise utilize University information and *IT resources* only for those activities they are specifically authorized and in a manner consistent with University policies, federal and state laws, and other applicable requirements.

III. PROCEDURES, FORMS, GUIDELINES, AND RESOURCES

A. Procedures

None.

B. Related Documents

The names and contact information of the persons with Program management responsibilities are provided in “IT Security Program Personnel and Contact Information.”

C. Related Administrative Policy Statements

The “IT Security Program” Administrative Policy Statement is the parent policy for a suite of policies addressing the protection of University information and information resources. The following policies are related to the roles and responsibilities of the University computing community:

- IT Security in Personnel Job Descriptions, Responsibilities, and Training
- IT Security in University Operations, Continuity, and Contracting

The Laws of the Regents, section 14.A.4 states that employees shall be responsible for the safekeeping and proper maintenance of university property in their charge. The administrative policy "Fiscal Code of Ethics" prohibits use of University property for personal gain.

The “Use of Electronic Mail” Administrative Policy Statement sets forth the appropriate use of University email and expectations for privacy in email communications.

D. Educational Resources

Educational resources including guides and training announcements are available on the [Office of Information Security](#) website.

IV. DEFINITIONS

Italicized terms used in this Administrative Policy Statement are defined in the Administrative Policy Statement *Dictionary*. Underlined terms specific to this policy, which are not found in other Administrative Policy Statements, are defined below.

V. CONTACTS

- A. The University Information Security Officer (ISO) will respond to questions and provide guidance regarding interpretation of this policy. Any exceptions to this policy must be approved by the University ISO.

VI. HISTORY

Amended: No amendments.

Initial Policy Effective: January 1, 2007

Supersedes: None.