



ASU Information Security Policy

Version 0.1
November 2008

1 Purpose

The ASU Information Security Policy establishes guidelines and standards for the preservation of the confidentiality, integrity and availability of University information resources. Additionally, the ASU Information Security Policy provides for the integrity of institutional processes and records and supports the University's compliance with state and federal laws, rules and regulations.

A third purpose of the ASU Information Security Policy is to create and implement a University Information Security Program and a University Information Security Committee in support of this policy.

2 Sources

Information Security Office

University Technology Office

Office of General Counsel

3 Applicability

All ASU employees, affiliates, vendors, service providers, sub-contractors, and students.

All computers and network systems owned by and/or administered within the University, including all platforms, all computer sizes and types, all applications and data contained on those systems, and all data storage systems and devices of any kind.

All information and data originating at or received by ASU in any form or format.

4 Policy

The University Technology Office is authorized to develop and create a University Information Security Program (Program) to establish, implement and maintain standards, protocols and procedures to preserve the confidentiality, integrity and security of information for the University. The Program will support the University's compliance with federal, state and ABOR laws, rules, regulations and policies and will support the implementation of information security best practices.

All individuals to whom this policy applies are responsible for protecting information in any kind of format, e.g. written, filmed, typed, recorded, printed, spoken, electronic, etc, from accidental or intentional unauthorized modification, destruction or disclosure in accordance with the information's sensitivity, criticality and value to the University. The protection includes an appropriate level of security regardless of the media on which it is stored, the manual or automated systems that process it, or the methods by which it is distributed. The appropriate level of security will be set forth in the Program and is based upon standards established by the Information Security Officer (ISO).

University administrators, including deans, department chairs, principal investigators, directors and managers, are responsible for ensuring the implementation and enforcement of this policy within their respective areas. The ISO is responsible for working with individuals and administrators to develop and implement prudent security procedures and standards in support of this policy and the Program. All computers and network systems implemented after the effective date of this policy should comply with this policy and the Program. Existing computers and network systems must be brought into compliance as soon as is practical.

The University Technology Counsel / Technical Advisory Group is responsible for the administration and oversight of the Program. The Committee will review and recommend information security procedures and standards to the University Technology Counsel and will provide guidance and support to the ISO. The composition of the Committee will at a minimum consist of the University Technology Officer, the ISO, a representative from the Office of General Counsel, the Provost's Office, Office of the President, ASUPD, ASU Libraries, the Office of Human Resources, 2 general academic members, and 2 general administration members.

In some circumstances, compliance with specific policy or Program requirements may not be immediately possible. Under those circumstances, academic or business units must confer with the Information Security Office to develop a plan for coming into compliance with this policy and the Program requirements within a reasonable amount of time.

Violation of this policy may lead to discipline as well as other applicable sanctions.