Purpose
The ASU Information Security Policy establishes the framework for the protection of ASU’s computing, internet, and communications resources, from accidental or intentional unauthorized access or damage, while also preserving the open information sharing requirements of its academic culture. This policy lays the foundation for a common understanding of information security at ASU based on the generally accepted principles of confidentiality, availability and integrity. Confidentiality limits information access to authorized users, integrity protects information against unauthorized modification and availability ensures that information is accessible when needed. Together these three principles ensure that university information can be used in support of the pursuit of the university’s goals of teaching, research, and service.

Additionally, the policy provides for the integrity of institutional processes and records and supports the university’s compliance with state and federal laws, rules and regulations. The ASU Information Security Policy outlines a University Information Security Program and a University Information Security Task Force in support of this policy.

Sources
Information Security Office
University Technology Office
Office of General Counsel

Applicability
This Standard applies to all Users of ASU’s computing, internet, and communications resources, including all students, faculty, staff (including student employees), contractors, vendors, consultants, temporary and other workers for ASU and its Component Units (Users).
This policy also applies to:
  o All computers and network systems owned by and/or administered within the university, including all platforms and all computer sizes and types.
  o All applications and data contained on those systems.
  o All data storage systems and devices whether local or hosted.
  o All devices connected to the university network including tablets, phones, etc.
  o Information and data originating at or received by ASU in any form or format.

Policy
Information created or maintained in the course of conducting university business is an institutional resource. This includes information created or maintained by ASU or its agents or affiliates. Although individuals, offices, departments, programs, or schools may have stewardship responsibilities for portions of university information assets and university records, the university itself retains ownership of, and responsibility for, university information.

The Information Security Office is authorized to maintain a university-wide Information Security Program to establish, implement and maintain standards, protocols and procedures to preserve the confidentiality, availability and integrity of university information. The Program will support the university’s compliance with all applicable legislative, regulatory, and contractual requirements concerning information security and promote effective information security practices. Details of ASU’s Information Security Program can be found on GetProtected, ASU’s Information Security website.

Individuals to whom this policy applies are responsible for protecting information in any format including but not limited to written, filmed, typed, recorded, printed, spoken, and electronic from unauthorized use, modification, destruction, or disclosure in accordance with the information’s sensitivity, criticality, and value to the University. The responsibility includes ensuring 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 information security is outlined in ACD 125: Computer, Internet, and Electronic Communications Information Management Policy, and supporting policies and standards, which include those maintained by the Information Security Office, the University Technology Office, Financial Services, and other policies found in the University Policy Manuals. In addition, all ASU faculty and staff are required to take information security awareness training within the first month of employment and annually thereafter. This training provides high-level guidance on minimum end-user training requirements.

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 Information Security Office is responsible for working with individuals, departments, and administrators to develop prudent security procedures and standards in support of this policy and the Program.

University Officers will appoint members of the Information Security Task Force to provide oversight for the Information Security Program. The Task Force will review and recommend information security initiatives, policies, standards, and procedures, as well as provide guidance and support to the Information Security Office. In addition to the ASU Chief Information Security Officer, the composition of the Task Force will at a minimum consist of a representative from the Office of General Counsel, the Provost’s Office, the Office of the CFO, the University Technology Office, and the Office of Knowledge Enterprise Development.

The Information Security Office provides standard language to be used in all information technology contracts where third parties will have access to sensitive university data. Purchasing may request a review of product or service contracts by the Information Security Office when access to sensitive data is involved or when an exception to standard requirements is requested.

**Violations and Enforcement**

Enforcement may include removal of systems from the ASU network or removal of access privileges to ASU’s computing, Internet and communication resources, until requirements are met. Violations of this Standard may lead to disciplinary actions or contract termination as applicable.

**Policy Revision**

This Policy is subject to review and revision at the direction of, and only after approval by, Chief Information Security Officer. To offer suggestions and/or recommendations, contact the ASU Information Security Office at infosec@asu.edu.

**References**

- ACD 125: Computer, Internet, and Electronic Communications Information Management Policy
- ASU Information Security Website
- ASU Policy Manuals
- ASU Information Security Program Overview
- ISO Policies/Standards/Procedures
- ASU Data Handling Standard
- ASU Incident Response Standard
- Information Security Task Force Charter
- Arizona Board of Regents Policy 9-201 (General Policy)
- Arizona Board of Regents Policy 9-202 (University Responsibilities)