

Policy Number: 9-201	Policy Name: General Policy
Policy Revision Dates:	Page 1

B. INFORMATION TECHNOLOGY SECURITY

9-201 General Policy

Information created, collected, or distributed by the universities and the Board is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. The universities and the Board must employ prudent information security policies, standards, and practices to minimize the risk to the integrity, confidentiality, and availability of information. Each university and the Board central office shall create and maintain an internal information security technology infrastructure to protect the confidentiality, availability, and integrity of information assets.

Policy Number: 9-202	Policy Name: University Responsibilities
Policy Revision Dates:	Page 1

9-202 University Responsibilities

- A. Each university president is responsible for assuring that appropriate and auditable information security controls are in place at the university for all university information resources and systems.
- B. Each university shall develop, implement, and maintain an information security program. Each university must submit its information security program to ATOC and to the Board for review and must report annually the university's progress on meeting its program goals.
- C. Each university shall develop, implement, and maintain a set of information security policies, and guidelines that are consistent with ABOR Information Security Program Guidelines and applicable law.
- D. Each university will establish detailed security standards that are consistent with the ABOR Information Security Program Guidelines.
- E. Each university shall establish an Information Security Office and designate an individual as Information Security Officer or Information Security Director. This individual will be responsible for the creation and implementation of an information security program that is consistent with ABOR Information Security Program Guidelines.
- F. Each university shall establish an Information Security Committee. The Committee will review and recommend information security policies and standards, and provide guidance and support to the Information Security Officer or Information Security Director for the implementation and maintenance of the Program.
- G. If a university determines that the probability of a security breach involving the acquisition of and access to personal information as defined in A.R.S. § 44-7501 (Security Breach Notification) is likely or has occurred, the Information Security Officer or Information Security Director shall report the incident promptly and in writing to the Executive Director of the Board. The Information Security Officer or Information Security Director shall also notify the Executive Director when the incident is closed. The incident closure report shall provide a description of the incident, including the nature of the incident and the numbers of individuals impacted, the incident handling process, a copy of the notification, if any, and the actions taken to prevent further breaches of security.