ARIZONA BOARD OF REGENTS
POLICY MANUAL

9-202 University Responsibilities

Revision Dates

6/15/2023 (effective 7/1/2023), 9/30/2022, 12/7/2012, 6/20/2008 (adopted)

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 that develops, implements, and maintains a set of information security policies, guidelines, and detailed security standards that are consistent with industry standards and applicable law. The information security program shall at a minimum:

1. Institute processes for policy and procedures that:

    a. Implement information technology (“IT”) security;

    b. Monitor and test implementation and practices;

    c. Develop metrics that report on IT security practices; and

    d. Remediate identified risks

2. Apply the processes developed in paragraph B.1 to areas that include, but are not limited to, the following:

    a. Employee security awareness and training.

    b. IT security controls that protect IT systems and data, and cover:

        i. Vulnerability management

        ii. Configuration management

        iii. Patch management

        iv. Web application development

        v. Log monitoring

        vi. Data classification

        vii. External parties management.

c. IT security governance that includes:

i. IT security strategic plan

ii. Documented roles and responsibilities

iii. Policies and guidance

iv. Monitoring processes

v. IT risk assessment

vi. Incident response.

C. "Industry Standards" as used in this policy means frameworks and standards that may include, but are not limited to, National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO).

D. 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 Industry Standards and applicable law.

E. Each university must report annually to the board Audit and Risk Management Committee on its information security program, including:

1. Metrics that measure the program's effectiveness;

2. Risk mitigation and remediation activities; and

3. Risk assessments, and whether the assessments have been shared as a part of the university-wide risk assessment that informs development of the annual audit plan.

F. In addition to complying with A.R.S. §§ 18-551 and 18-552, if a university determines that an information technology system is experiencing or has experienced a "security system breach", as defined in A.R.S. § 18-551, involving the unauthorized acquisition of and unauthorized access to personal information, which meets the threshold in A.R.S. § 18-552.B.2., the information security officer or information security director shall report the incident promptly and in writing to the board's executive director and the board chair. The information security officer or information security director shall also notify the board's executive director and the board chair 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.

Policy History

6/20/2008 Approved by the Board on second reading.

12/7/2012 Policy revision approved by the Board on second reading.

9/30/2022 Policy revision approved by the Board on second reading.

6/15/2023 Policy revision approved by the Board on second reading to be effective 7/1/2023.

Related Information