

CHAPTER IX	
<u>INFORMATION TECHNOLOGY</u>	
A. INFORMATION TECHNOLOGY PLANNING AND OVERSIGHT PROCESSES	9-101
Arizona Board of Regents Technology Oversight Committee Charter (ATOC)	9-101
Definitions	9-102
Tri-University Information Technology Architecture	9-103
Information Technology Strategic Plans	9-104
Project Approval Process	9-105
Quarterly Reports	9-106
Annual Reports	9-107
Budget Overrun Protocol	9-108
Regent's IT Innovation Fund	9-109
B. INFORMATION TECHNOLOGY SECURITY	9-201
General Policy	9-201
University Responsibilities	9-202
C. ARIZONA UNIVERSITIES NETWORK (AZUN) PLANNING, BUDGETING AND OVERSIGHT PROCESSES	9-301
AZUN Planning	9-301
AZUN Management	9-302
AZUN Budgeting	9-303
AZUN Annual Reports	9-304
Arizona Regents Reach Out Grants	9-305

Policy Number: 9-101	Policy Name: Arizona Board of Regents Technology Oversight Committee Charter (ATOC)
Policy Revision Dates:	Page 1

CHAPTER IX – INFORMATION TECHNOLOGY

A. INFORMATION TECHNOLOGY PLANNING AND OVERSIGHT PROCESSES

9-101 Arizona Board of Regents Technology Oversight Committee Charter (ATOC)

- A. The purpose of ATOC is to provide oversight for major Information Technology (IT) initiatives at the Arizona University System (AUS) campuses. This oversight involves reviewing and approving plans for major campus investments to ensure that they are effectively planned and managed and that they are aligned with major ABOR and university goals.

- B. The focus of ATOC will be to:
 1. Guide, establish, and approve IT strategic plans, technology-based standards, applications and services in support of future ABOR and University needs.
 2. Operate as a forum for the discussion of major issues related to technology, collaborative applications and IT services.
 3. Evaluate, approve and monitor significant systems development, collaborative projects and technology infrastructure expenditures in excess of \$1 million.
 4. Facilitate appropriate technology collaboration in support of ABOR’s mission and business goals.
 5. Provide policy direction for the Arizona Universities Network (AZUN) and approve AZUN annual program budgets.

Policy Number: 9-102	Policy Name: Definitions
Policy Revision Dates:	Page 1

9-102 Definitions

Definitions for this Chapter are included in the ABOR Information Security Program Guidelines. These Guidelines may be amended as necessary by the ATOC without the need for full Board review.

Policy Number: 9-103	Policy Name: Tri-University Information Technology Architecture
Policy Revision Dates:	Page 1

9-103 Tri-University Information Technology Architecture

The universities will participate in the creation and development of a Tri-University IT Architecture to guide the design, implementation, maintenance and organization of information technology management at each institution. The Tri-University IT Architecture will be submitted to the ATOC for review and approval.

Policy Number: 9-104	Policy Name: Information Technology Strategic Plans
Policy Revision Dates:	Page 1

9-104 Information Technology Strategic Plans

- A. University IT and AZUN strategic plans should identify major initiatives and costs and should align with ABOR System and University five-year plans. These strategic plans should also take into account best practices, the Tri-University IT Architecture, and the ABOR Information Security Program Guidelines.
- B. The plans should identify the current status of university IT initiatives and plans for achieving future initiatives including benefits, costs, time frames, resources, sponsorship, and user involvement.
- C. The IT Strategic Plans will be submitted to ATOC for review and approval.
- D. IT strategic plans will follow a common format approved in advance by the ABOR Executive Director.

Policy Number: 9-105	Policy Name: Project Approval Process
Policy Revision Dates:	Page 1

9-105 Project Approval Process

- A. IT project budget of \$100K-\$1M:
 - 1. Requires approval of university president and CIO;
 - 2. University must report to ATOC quarterly following university president's approval;
 - 3. University must report status annually with the IT Strategic Plan.

- B. IT project budget of \$1M-\$10M:
 - 1. University must complete IT Project Justification Summary and submit it for ATOC approval;
 - 2. Prior ATOC approval is necessary before project is initiated.
 - 3. University must report status annually with the IT Strategic Plan or quarterly at the ATOC's request.

- C. IT project budget over \$10M:
 - 1. University must submit complete IT Project Justification Summary and submit it for ATOC review and recommendation to the Board;
 - 2. Prior ATOC review and Board approval is necessary before project is initiated.
 - 3. University must report on project status to ATOC quarterly;
 - 4. Project may be subject to external monitoring if required by ATOC.

- D. Project Justification Summaries should summarize the anticipated project budget for five years; projects may not be divided into smaller projects to affect the approval process.

- E. The Board may retain independent consultants to monitor significant projects. All projects are subject to audit.

- F. If a University president believes that an emergency situation requires immediate action, the president may contact the Chair of ATOC or the Executive Director of the Board to request either a special meeting of ATOC or permission to take immediate action and submit a Project Justification Summary Sheet for ATOC review and ATOC or Board ratification at the next regularly scheduled meeting according to the preceding dollar thresholds.

Policy Number: 9-106	Policy Name: Quarterly Reports
Policy Revision Dates:	Page 1

9-106 Quarterly Reports

Every quarter, each university must provide a written report to ATOC showing the status of all active and pending IT projects between \$100,000 to \$1 million that have been approved at the university level. The format for quarterly reports must be approved by the Executive Director of the Board.

Policy Number: 9-107	Policy Name: Annual Reports
Policy Revision Dates:	Page 1

9-107 Annual Reports

- A. Each university must submit an annual report to ATOC in a format approved by the Executive Director of the Board to report on expenditures and other issues relating to capital, operations, and personnel.
- B. Each university will provide an annual expense report to ATOC for capital, operations, and personnel expenses. The report will be provided to ATOC in a fall meeting to be determined by ATOC in a format approved by the Executive Director of the Board and will reflect data for the prior year.

Policy Number: 9-108	Policy Name: Budget Overrun Protocol
Policy Revision Dates:	Page 1

9-108 Budget Overrun Protocol

If an IT project over \$1 million is anticipated to exceed the Board approved budget by 25% or \$1 million dollars, whichever is less, the project must be resubmitted to the ATOC Committee for review and to ATOC or the Board for approval according to the preceding dollar thresholds.

Policy Number: 9-109	Policy Name: Regent's IT Innovation Fund
Policy Revision Dates:	Page 1

9-109 Regent's IT Innovation Fund

The Regent's IT Innovation Fund primarily supports central office and university collaborative IT projects. Requests for ATOC approval for the use of these funds are to be submitted on a form approved by the Executive Director of the Board. Annual progress and expenditure reports for collaborative projects will be submitted to ATOC at the same time as the IT annual reports.

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.

Policy Number: 9-301	Policy Name: AZUN Planning
Policy Revision Dates:	Page 1

C. ARIZONA UNIVERSITIES NETWORK (AZUN) PLANNING, BUDGETING AND OVERSIGHT PROCESSES

9-301 AZUN Planning

The principal activities of AZUN are to support e-learning, workforce development program priorities and the management and development of the tri-university AZUN web portal. The web portal provides access to academic programs and courses that are available on-line from the universities. AZUN is funded annually from TRIF sources.

Policy Number: 9-302	Policy Name: AZUN Management
Policy Revision Dates:	Page 1

9-302 AZUN Management

The management of AZUN is delegated to Northern Arizona University. The Board retains policy and budgetary oversight of AZUN activity by requiring periodic reporting and detailed annual budgetary approval by ATOC.

Policy Number: 9-303	Policy Name: AZUN Budgeting
Policy Revision Dates:	Page 1

9-303 AZUN Budgeting

Annually AZUN will submit a detailed program budget request for approval by the ATOC.

Policy Number: 9-304	Policy Name: AZUN Annual Reports
Policy Revision Dates:	Page 1

9-304 AZUN Annual Reports

AZUN will provide an annual report that includes: goals, program performance evaluations and measures, and summary expenditure data.

Policy Number: 9-305	Policy Name: Arizona Regents Reach Out Grants
Policy Revision Dates:	Page 1

9-305 Arizona Regents Reach Out Grants

Arizona Regents Reach Out (ARRO) grants are annual grants provided by the Board to promote and support e-learning initiatives.