Information Technology Governance Policy

Policy 916

1 Introduction

Appalachian State University’s Information Technology Services (IT) and information resource needs continually evolve as new challenges, opportunities, and technologies emerge. The University adopts this policy to:

1. Align our IT governance objectives and comply with the University of North Carolina Information Technology Governance Policy, 1400.1;
2. Designate the Chief Information Officer as the position responsible for overseeing the information technology governance program and ensuring the establishment and proper implementation and operation of the information technology governance program framework and principles across all areas of campus IT;
3. Outline an IT governance program that ensures information technology solutions are cost effective, strategically aligned with institutional goals, and identify and minimize risk to the institution;
4. Encourage information technology collaboration and shared service agreements between the University Information Technology units and staff, and where appropriate, between and among, University of North Carolina institutions and the System Office; and
5. Ensure the objectives, information, and standards established within this policy have a broad campus distribution and adoption across all areas of campus IT.

2 Scope

2.1 This policy applies to all Appalachian State University employees, students, and affiliates.

3 Definitions

3.1 Information Resources

Information resources are information owned or possessed by the University, or related to the business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information.

3.2 Institutional Data

Institutional data is data that originates in an academic or administrative system, and data contained within the University data warehouse.

3.3 Information Technology

Information technology is the hardware and software resources owned, leased, or used by the University and its partners to store, process or transmit University information. Information technology is a subset of the University’s information resources.

3.4 Information Technology Governance

Information technology governance are the policies, standards, structures, processes, and guidance established to ensure that the University’s information technology supports the mission, goals, and objectives of the University; that information technology and information resources are managed in accordance with standards and policies; and that risks and threats to information technology and information resources are appropriately and effectively identified and addressed. IT governance encompasses the planning, prioritization, funding, evaluation, auditing, and security of information technology and information resources at the University.

3.5 Periodic
Periodic means occurring at a frequency deemed appropriate based on an on-going assessment of associated risks.

3.6 Information Technology Policies

IT Policies are University policies that articulate the University’s values, principles, strategies, and positions relative to Information Technology.

3.7 Information Technology Standards

IT Standards are documentation that establish requirements and/or processes that provide a reliable basis for shared expectations on how work will be conducted, and facilitate compliance with University policies, applicable laws and regulations.

3.8 Information Technology Guidelines

IT Guidelines are documentation that recommends practices to streamline processes and/or reduce risk. IT guidelines are not mandatory.

3.9 Information Technology Projects

IT Projects are temporary endeavors to 1) introduce new campus applications, services, IT policies and standards, and 2) implement significant changes to existing infrastructure, applications and enterprise systems, policies and standards.

4 Policy and Procedure Statements

4.1 Information Technology Governance Program

4.1.1 In alignment and compliance with UNC Policy 1400.1, the Chancellor vests the Chief Information Officer with the authority and responsibility to oversee an IT governance program that includes central and distributed information technology units and staff for consistent planning, prioritizing, funding, evaluating, and auditing of information resources and technology in order to meet:

1. Internal and external requirements for the protection of institutional data and systems, and
2. The need to innovate and adopt new processes and systems to fulfill the University’s mission.

4.1.2 The IT governance program includes IT policies, IT standards and IT guidelines that apply to all University units and staff.

1. Policies and/or standards including, but not limited, to Information Security, Data Management, Risk Management, Encryption, Disaster Recovery, Software and Hardware standards, Acquisition of IT consulting and contracting services, Networking, Wireless Technologies, and personal devices will be developed and maintained as part of the IT governance program.
2. Impacted campus entities, including, at minimum, the IT Implementation Group and the IT Board of Directors will review proposed IT policies and standards.

4.1.3 Effective coordination and communication within and among IT units, IT staff, and campus is a critical success factor of IT governance.

1. The Chief Information Officer, in conjunction with the IT Executive Council, IT Board of Directors, and IT Implementation Group, will develop a quarterly report of IT projects and share relevant information to campus through outreach and website publications.
2. Information regarding new and revised IT policies, standards, and guidelines will be maintained on an IT website.

4.2 Roles and Responsibilities

4.2.1 The Chancellor and Chancellor’s Cabinet shall be responsible for:

1. Providing guidance concerning institutional risk tolerance levels.
2. Periodically reviewing the University’s IT Governance program.

4.2.2 The Chief Information Officer shall be responsible for:
1. Developing, implementing and overseeing the IT governance program that encompasses distributed, central and functional IT units and staff.
2. Requesting the Chancellor's approval of IT policies.
3. Developing, approving, and enforcing IT standards and guidelines based on recommendations from IT governance groups and the Chief Information Security Officer.
4. Directing the periodic review of policies, standards and procedures to identify gaps and develop action plans to address gaps.
5. Periodically reviewing and updating IT governance principles, guidelines and standards to ensure effective operation of the IT governance program.
6. Publishing information about the University's IT governance program. This information will include membership, policies, standards, and high impact projects, on a University website for the sake of transparency and to promote business and IT synergy.
7. Identifying exceptions that are inconsistent with IT Governance principles, standards and correcting deficiencies.

4.2.3 The IT Executive Council is comprised of leadership from each University division and serves as a forum to discuss IT issues, resources, and challenges. The IT Executive Council is responsible for the following:

1. Recommending changes to IT policies and standards.
2. Providing oversight of the IT governance program and reviewing exceptions that are inconsistent with IT Governance principles and standards.
3. Reviewing and approving IT standards identified by the Chief Information Officer to have a significant institutional impact.
4. Approving a prioritization model for evaluating IT projects.
5. Making strategic project decisions regarding funding, risk and business process changes.
6. Reviewing, advising and accepting a quarterly report of IT projects.

4.2.4 The IT Governance Board of Directors is comprised of directors of central and distributed IT units, representation from the Faculty Senate, and divisional Directors and/or Associate Vice Chancellors with significant numbers of IT employees. The IT Governance Board of Directors shall be responsible for the following:

1. Reporting and recommending IT projects, reviewing prioritization of IT projects, and accepting a quarterly report of IT projects.
2. Reviewing and advising on IT policy and standards.
3. Approving operational changes with limited campus impact, and approving Technical Advisory Groups.
4. Functioning as the governance liaison to their respective areas or division. As a divisional/unit governance liaison, the IT Governance Board of Directors members will:
   1. share information regarding significant new and ongoing divisional/unit information technology efforts in order to encourage collaboration and shared service agreements, and ensure that efforts are strategically aligned with institutional goals and risk mitigation efforts, and
   2. disseminate information regarding IT Board of Directors efforts within their division/unit.

4.2.5 The IT Implementation Group is comprised of managers and IT staff within central, distributed and key functional areas. The IT Implementation Group shall be responsible for:

1. Recommending standards, guidelines, projects and procedures to ensure the effective and efficient use of IT.
2. Reviewing proposed technology changes, IT projects, IT policies, standards and guidelines for impact, feasibility, resource needs, and developing implementation plans.
3. Advising on the development of a quarterly project report of IT projects.

4.2.6 Technical Advisory Groups are University committees, councils and working groups that focus on assuring that information resources and technology needs are met to support an aspect of the University mission. The Chief Information Officer, or delegate, provides information on IT projects and initiatives to Technical Advisory Groups on a quarterly basis to coordinate governance to fulfill the University’s mission. Technical Advisory Groups shall be responsible for:

1. Requesting IT projects to meet institutional needs.

4.2.7 The Data Stewards Council is comprised of University employees with planning and management responsibility for defined institutional datasets. The Data Stewards Council shall be responsible for:

1. Overseeing the development and maintenance of standards needed to ensure the consistent treatment of institutional data as well as periodically reviewing and reporting on the effectiveness of University data management practices.
2. Ensuring that the management of individual data sets conforms to relevant University policies and stewards.
3. Coordinating and resolving stewardship issues and data definitions of data elements that cross multiple functional units.

5 Additional References

1. Information Security Policy
2. Data Management Standard
3. Information Security Risk Management Standard
4. Secure Data Handling Standards
5. IT Policy, Standards and Guidelines Website

6 Authority

UNC Policy Manual 1400.1 - Information Technology Governance
UNC Policy Manual 1400.2 - Information Security

7 Contact Information

The Office of the Chief Information Officer - (828)262-6278

8 Original Effective Date

January 29, 2019

9 Revision Dates