Information Security Policy

Policy 903

1 Introduction

The purpose of this policy is to outline the framework for the University's comprehensive Information Security Program to help safeguard the confidentiality, integrity, and availability of campus Information Resources, and comply with federal and state law, and UNC System policies.

2 Scope

This policy applies to all Appalachian State University employees, students, vendors and visitors.

3 Definitions

3.1 Information Security

The preservation of the confidentiality, integrity and availability of Information Resources and Institutional Data.

3.2 Information Security Program

Policies, assessments, protocols, and training designed to govern the security of Information Resources.

3.3 Information Resources

Same meaning as defined in Appalachian Pollicy 901 - IT Governance Policy.

3.4 Control

The management of risk which can be of an administrative, technical, management, or legal nature. Examples include policies, procedures, guidelines, practices or organizational structures.

3.5 Information Security Event

An identified occurrence of a system, service, or network state indicating a possible breach of Information Security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

3.6 Information Security Incident

An unwanted or unexpected Information Security Event that has a significant probability of compromising business operations and threatening Information Security.

3.7 International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

Independent international organizations responsible for the creation of industry technical and administrative security standards.

4 Policy and Procedure Statements

4.1 Information Security Program

The University shall develop, implement, and maintain a comprehensive Information Security Program (the "Program"). The Program will be updated on a periodic basis or as necessitated by significant changes to the University's mission, major initiatives, or opportunities. The development of the plan will be guided by the following elements:

a. ISO/IEC 27002 - The Program shall be guided and informed by the ISO/IEC 27002 standard, adopted as the common security framework baseline for campuses of the UNC system;
b. Legal, Contractual, and Policy Requirements - In relation to the management and protection of Information Resources, the

University shall conduct all business in accord with relevant federal and state law, and UNC System policies; and
c. Proactive Risk Management - The Program shall be driven by the identification, assessment, communication, and cost-effective treatment of risks related to University Information Resources.

4.2 Governance, Coordination, and Security Services

4.2.1 Board of Trustees Audit Committee

Appalachian's Board of Trustees Audit Committee will review and provide oversight of Information Security on at least an annual basis including, but not limited to, emerging Information Security matters, institutional Program activities, information technology security Controls, and risk assessments.

4.2.2 Information Security Advisory Council

To ensure the Program is aligned with the University's mission, values, and operational needs, the Chancellor will appoint a University Information Security Advisory Council to oversee the collaborative development of the plan and associated policies, major initiatives, and campus security solutions.

4.2.3 Information Security Liaisons

To ensure that campus units are informed about security initiatives, practices, and requirements, University units that maintain and manage their own Information Technology will appoint Information Security Liaisons to act as central points of contact for communication and coordination with the ITS - Office of Information Security.

4.2.4 ITS - Office of Information Security

The ITS Office of Information Security shall be responsible for providing Information Security services that help identify risks, establish protective measures, and validate conformance with relevant University Information Security policies and standards.

4.3 Roles and Responsibilities

4.3.1 Shared Responsibilities

Information Security is a shared responsibility. All employees, students, visitors and vendors of the University share in the responsibility to help protect University Information Resources. The roles and responsibilities for University Information Security include:

4.3.2 Chancellor and Chancellor's Cabinet

The Chancellor and Chancellor's Cabinet shall be responsible for:

a. Approval of the University's Information Security policy;
b. Providing executive oversight and support of the Information Security Program;
c. Providing guidance concerning institutional risk tolerance levels;
d. Providing resources to meet approved security objectives; and
e. Periodically reviewing the University's Information Security posture.

4.3.3 The Chief Information Officer

The Chief Information Officer shall be responsible for oversight of Information Security in accordance with UNC System policies, and has authority and accountability for:

a. The campus-wide adoption, implementation, and enforcement of the Information Security Program;
b. Deploying all reasonable measures to maintain the confidentiality, integrity, and availability of Information Resources;
c. Periodically reporting Information Security posture to the Chancellor and Chancellor's Cabinet and Board of Trustees Audit Committee; and
d. Delegating select authority to the Chief Information Security Officer and/or other institutional officers as needed to meet the objectives listed elsewhere in this policy.

4.3.4 Chief Information Security Officer

The Chief Information Security Officer shall be responsible for:

a. Leading the development and execution of the Program;
b. Facilitating Information Security governance and collaboration;
c. Advising the Chief Information Officer and senior leadership on security needs and resource investments; and
d. Development of Information Security policies, standards, and guidelines.

4.3.5 Deans and Department Heads

Deans and Department Heads shall be responsible for:

a. Ensuring that units adhere to Information Security policies and standards; and
b. Ensuring that reporting staff receives any required security training.

4.3.6 University Employees and Students

All University employees and students shall be responsible for:

a. Awareness and adherence to Information Security policies, standards, and guidelines;
b. Attending any required Information Security training; and
c. Prompt reporting of Information Security Events and Incidents to Information Technology Services without delay.

4.3.7 Vendors

Complying with all federal and state laws, UNC System policies, Appalachian policies, and contractual obligations with the University concerning the protection of information resources and information technology.

5 Additional References

Appalachian Policy 503.8 - Payment Card Services Policy
Appalachian Policy 901 - Information Technology Governance Policy
Appalachian Policy 902 - Data Governance Policy

6 Authority

1. Enterprise Password Management Standard
2. Information Security Risk Management Standard
3. Secure Data Handling Standards
4. Payment Card Industry Data Security Standard
5. UNC Policy Manual, Chapter 100.1, Section 502s
6. UNC Policy Manual - 1400.2 Information Security
7. Gramm-Leach-Bliley Act (Public Law 106-102; 113 Stat. 1338) 16 CFR Part 314
8. Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191; 110 Stat. 1936) 45 CFR Part 164

7 Contact Information

Office of the Chief Information Officer (828-262-6278)
Chief Information Security Officer (828-262-6277)

8 Original Effective Date

March 16, 2015

9 Revision Dates

November 28, 2018
December 7, 2020