Information Security Policy

Policy 903

1 Introduction

1.1 Appalachian State University will develop, implement, and maintain a comprehensive Information Security Program to help safeguard the confidentiality, integrity, and availability of campus information resources and address security requirements defined by University of North Carolina policies, state and federal laws, and relevant contractual obligations.

2 Scope

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

3 Definitions

3.1 Information Security

   Information Security is the preservation of confidentiality, integrity and availability of information.

3.2 Confidentiality

   Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.3 Availability

   Availability is the property that information is accessible and usable upon demand by an authorized person or entity.

3.4 Integrity

   Integrity is the property that information is accurate and complete.

3.5 Risk

   In the context of Information Security, risk is the exposure to potential reduction of confidentiality, integrity, and availability of information assets such as information systems, data, user credentials, and other computing resources.

3.6 Control

   A control is a means of managing risk which can be of an administrative, technical, management, or legal nature. Examples include policies, procedures, guidelines, practices or organizational structures.

3.7 Information Security Program

   “Information Security Program” means policies, assessments, protocols, and trainings designed to govern the storage, accessibility, and security of information resources. (UNC Information Security Policy 1400.2, Section IIA)

3.8 Information Processing Facilities

   Any information processing system, service, or infrastructure, or the physical facilities housing them.

3.9 Information Resources

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

3.10 Information Security Event
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.

3.11 Information Security Incident

Unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

3.12 Data Maintenance

The action of managing or editing the data inside an administrative system for the purpose of doing business at the University.

3.13 Data Inquiry

The action of querying data from an environment designed for that purpose with the intent of informing and influencing decision making.

3.14 ISO

“ISO” refers to the International Organization for Standardization.

3.15 GLBA

“GLBA” refers to the Gramm-Leach-Bliley Act. \(\text{Public Law 106-102; 113 Stat. 1338}\)

3.16 HIPAA

“HIPAA” refers to the Health Insurance Portability and Accountability Act of 1996. \(\text{Public Law 104-191; 110 Stat. 1936}\)

3.17 CFR

“CFR” refers to the Code of Federal Regulations.

3.18 PCI-DSS

“PCI-DSS” refers to the Payment Card Industry Data Security Standard.

3.19 University

“University” means Appalachian State University.

4 Policy and Procedure Statements

4.1 Information Security Program

As mandated by UNC Policy 1400.2, and consistent with the roles and responsibilities outlined in Section 4.3 of this Policy, the University shall develop, implement, and maintain a comprehensive Information Security Program. This 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:

4.1.1 ISO/IEC 27002:2013 - The University's Information Security Program shall be guided and informed by the ISO/IEC 27002 standard, adopted as the common security framework baseline for campuses of the University of North Carolina (UNC) system.

4.1.2 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 University of North Carolina policies, state laws, federal laws, and contractual requirements.

4.1.3 Proactive Risk Management - The development of the University's Information Security 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 - As mandated by UNC Policy 1400.2, the University’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 information security program activities, information technology security controls, and risk assessments. ([UNC Information Security Policy 1400.2, Sections V.A, B, and C](#))

4.2.2 Information Security Advisory Council - To ensure the Information Security Program is aligned with the University’s mission, values, and operational needs, a University Information Security Advisory Council will be formed 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

Information Security is a shared responsibility. All employees of the University share in the responsibility to help protect University information resources.

The roles and responsibilities for University Information Security include:

4.3.1 Chancellor and Chancellor’s Cabinet - The Chancellor and Chancellor’s Cabinet shall be responsible for:

1. Approval of the University’s Information Security policy.
2. Providing executive oversight and support of the Information Security Program.
3. Providing guidance concerning institutional risk tolerance levels.
4. Providing resources to meet approved security objectives.
5. Periodically reviewing the University’s information security posture.

4.3.2 The Chief Information Officer - As defined in the UNC Information Security Policy (1400.2), the Chief Information Officer shall have authority and accountability for:

1. The campus-wide adoption, implementation, and enforcement of the Information Security Program.
2. Deploying all reasonable measures to maintain the confidentiality, integrity, and availability of information resources.
3. Periodically reporting information security posture to the Chancellor and Chancellor’s Cabinet and Board of Trustees Audit Committee.
4. 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.

4.3.3 Chief Information Security Officer - The Chief Information Security Officer shall be responsible for:

1. Leading the development and execution of the University’s security program.
2. Facilitating information security governance and collaboration.
3. Advising the Chief Information Officer and senior leadership on security needs and resource investments.

4.3.4 Deans and Department Heads - Deans and Department Heads shall be responsible for:

1. Ensuring that units adhere to information security policies and standards.
2. Ensuring that reporting staff receives any required security training.

4.3.5 University Employees - All University employees shall be responsible for:

1. Awareness and adherence to information security policies and standards.
2. Attending any required information security training.

4.4 Key Control Requirements

To address relevant policy, legal, and contractual obligations, the following key security control requirements will be addressed through existing controls, compensating controls, or prioritized implementation planning consistent with available resources.

4.4.1 Risk Management
1. Regular identification and analysis of risks will be performed for information assets identified as having a high level of importance.

2. Risk treatment options, including any cost-effective controls, will be analyzed and identified.

3. Applicable risks and treatment options will be communicated on a regular basis for decision review. Reference: ISO 27002:2013-6.1.1; GLBA: 16 CFR §314.4; HIPAA: 45 CFR §164.308(a)(1)(ii)(A); PCI-DSS 3.2-12.2, UNC Information Security Policy (1400.2, Section III)

4.4.2 Human Resource Security

1. Screening/Background Checks - Prospective employees who receive an offer of employment will be vetted via a background check including a criminal background investigation. Reference: ISO 27002:2013-7.1.1; HIPAA: 45 CFR §164.308(a)(3)(ii)(B); PCI-DSS 3.2-12.7

2. Security Awareness Training - All University employees will receive regular security awareness training in addition to any specific training associated with job responsibilities and employee roles. Reference: ISO 27002:2013-7.2.2, PCI-DSS 3.2-12.6

3. Disciplinary Process - Employee disciplinary processes will include applicable provisions to cover any egregious violations of approved information security policies or requirements. Reference: ISO 27002:2013 - 7.2.3; HIPAA: 45 CFR §164.308(a)(1)(ii)(C)

4. Termination of Employment - Access to University information resources, work areas, and processing facilities will be revoked and assets returned upon full termination of employment with University. Retirees may retain an institutional email account and associated services to maintain connection to campus. Reference: ISO 27002:2013-7.3, 8.1.4; HIPAA: 45 CFR § 164.308(a)(3)(ii)(C); PCI-DSS 3.2: 8.1.3; 9.3

4.4.3 Asset Management

1. Data Governance - All institutional data will be considered the property of the University and will be treated as an asset. A data management structure will be established that defines responsibilities for secure and effective management of institutional data.

2. Data Classification – The University will adopt a consistent data classification scheme that takes into account associated business needs and risks related to sharing or restricting information. Reference: ISO 27002:2013-8.2

3. Acceptable Use and Security Requirements - Appropriate utilization of University information assets will be clearly defined, including secure practices for handling data classified as sensitive. Reference: ISO 27002:2013-8.1.3,8.2.2

4. Inventory of Important Assets - An inventory of all information assets that have a high level of importance will be maintained and indicate their owner, location, and management information. Reference: ISO 27002:2013-8.1.1,8.1.2; HIPAA: 45 CFR §164.310(d)(2)(iii)

5. Information Asset Transfer and Destruction - Information assets will be reliably transferred and any data they contain rendered unreadable prior to transfer to another employee, sale or other disposition. Reference: ISO 27002:2013-8.1.4,8.3.2,11.2.7; HIPAA: 45 CFR §164.310(d)(2)(i),§164.310(d)(2)(ii); PCI-DSS 3.2-9.8

4.4.4 Access Control

1. Role Based Access Control - University information asset owners will define appropriate roles associated with the fulfillment of legitimate business needs. These roles should be defined based on two functions:
   1. Data Maintenance Roles - The access for data maintenance in administrative systems will be determined based on the employee position and location, and will be governed by the business requirements.
   2. Data Inquiry Roles - The access for data inquiry will be determined by the required data set and associated data classification level, and will be governed by the data steward assigned the requested data set. These roles will have associated access control rules, access rights, and restrictions that provide a sufficient degree of access needed to efficiently accomplish these business needs. Assignments to these roles should be periodically reviewed. Reference: ISO 27002:2013-9.1; HIPAA: 45 CFR §164.312(a)(1); PCI-DSS 3.2-7.1

2. Network Access Control - Local and remote access to University networks and information services will be limited to authorized individuals with legitimate business needs. Reference: ISO 27002:2013-9.1.2; HIPAA: 45 CFR §164.312(a)(1); PCI-DSS 3.0.9.1.2

3. User Access Management - Formal user provisioning and deprovisioning processes will be implemented to ensure that creation of new accounts is authorized, users are uniquely identified, redundant userIDs are periodically removed, and that userIDs are disabled when no longer required. Reference: ISO 27002:2013-9.2.1,9.2.2; HIPAA: 45 CFR §164.312(a)(2)(i), §164.312(a)(2)(d); PCI-DSS 3.2-8.1.2

4. Management of Privileged Access - Privileged access rights will be appropriately evaluated, approved, periodically reviewed, and limited to only those users and applications with legitimate and sufficient business need. Reference: ISO 27002:2013-9.2.3; PCI-DSS 3.2-7.1

5. Password Management - Passwords used to access University resources will be established and managed in a formally approved and consistently secure manner. Reference: ISO 27002:2013-9.2.4, HIPAA: 45 CFR §164.308(a)(5)(ii)(D)

6. Secure Logon - Common secure logon practices will be defined and implemented to ensure that means of access to University systems and applications effectively minimize the risks of unauthorized access threats. Reference: ISO 27002:2013-9.4.2; HIPAA: 45 CFR §164.312(a)(2)(iii)
4.4.8 Communications Security

1. Network Service Authority - The management and provisioning of University network connections, services, and devices will be limited to authorized staff only. Reference: ISO 27002:2013-13.1.1.1,13.1.1.2
2. Network Filtering - Network traffic traversing University owned networks will be filtered to address any appreciable risks and to preserve equitable availability of University network resources. Reference: ISO 27002:2013-13.1.1.g,13.1.2; GLBA: 16 CFR §314.4(2); PCI-DSS 3.2-1.1
3. Network Attack Detection and Prevention - Network traffic traversing University owned networks will be inspected for active attacks against University information assets. Interdiction capabilities will be maintained to effectively block attacks that present appreciable risks to the University. Reference: ISO 27002:2013-13.1.1.d; GLBA: 16 CFR §314.4(3); PCI-DSS 3.2-1.3,1.4
4.4.13 Compliance Management

4.4.11 Information Security Incident Management

4.4.10 Supplier Relationship

4.4.9 System Acquisition, Development and Maintenance

1. Security Requirements Analysis - The development and acquisition of information systems will include the regular evaluation of security requirements in the earliest possible stages of related information system projects. Reference: ISO 27002:2013-14.1.1

2. Secure Development - Secure program techniques and modeling methods will be employed to ensure that coding practices adhere to best practices to limit potential for abuse. Reference: ISO 27002:2013-14.2.1

3. System Change Control - Change control procedures will be documented and enforced to ensure the confidentiality, integrity, and availability of information systems throughout maintenance efforts. Reference: ISO 27002:2013-14.2.2

4. System Security Testing - System acceptance testing will include security testing and validation of effectiveness of controls related to any identified information security requirements. Reference: ISO 27002:2013-14.2.2

5. Test data - If viable options are available, data that contains sensitive information will not be used for system or application testing purposes. Test systems that do contain this data must adhere to common data security standards. Reference: ISO 27002:2013-14.2.8

4.4.12 Business Continuity Management

1. Information Security Continuity - Planning will be undertaken to ensure that appropriate levels of information security protection measures are maintained during emergencies or other adverse events. Periodic verification of these plans will be performed on an annual basis. Reference: ISO 27002:2013-17.1.1, 17.1.2, 171.3

2. Redundant Information Processing Facilities - Information processing facilities will be implemented with redundancy sufficient to meet identified and documented availability needs. Reference: ISO 27002:2013-17.2

4.4.13 Compliance Management

1. Identification of Compliance Requirements - Regular periodic review will be conducted to ensure that relevant policies, legal and contractual requirements are identified for the University and relevant information systems. Reference: ISO 27002:2013-18.1.1

2. Intellectual Property Rights - Procedures will be implemented to ensure compliance with applicable legal, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products. Reference: ISO
Protection of Records - University records will be protected from loss, destruction, falsification, and unauthorized release in accordance with legal, regulatory, and contractual business requirements. Reference: ISO 27002:2013-18.1.2

Privacy and Protection of Personally Identifiable Information - The privacy and protection of personally identifiable information will be ensured as required in relevant legal and regulatory frameworks. Reference: ISO 27002:2013-18.1.3

4.4.14 Information Security Review

1. Independent Review of Information Security - Assessment of the University’s approach to and management of information security objectives will be performed periodically by a qualified independent third party. Reference: ISO 27002:2013-18.2.1

2. Compliance with Security Policies and Standards - Periodic review will be conducted to review the adherence of University units and employees to applicable information security policies and standards. Reference: ISO 27002:2013-18.2.2

3. Technical Compliance Evaluations - Periodic technical evaluations, including both automated and manual security assessments, should be performed to ensure that technical controls and security measures adhere to applicable information security policies and standards. Reference: ISO 27002:2013-18.2.3

5 Additional References

- Payment Card Industry Data Security Standard
- Data Management Standard
- Enterprise Password Management Standard
- Payment Card Services Policy
- Information Security Risk Management Standard
- Secure Data Handling Standards

6 Authority

- UNC Policy Manual, Chapter 100.1, Section 502
- UNC Policy Manual - 1400.2 Information Security
- Gramm-Leach-Bliley Act (Public Law 106-102; 113 Stat. 1338) 16 CFR Part 314

7 Contact Information

ITS Office of Information Security, 828-262-6277

8 Original Effective Date

March 16, 2015

9 Revision Dates

November 28, 2018