Information Security Policy

Policy 903

1 Introduction

1.1 Appalachian State University will develop, implement, and maintain a comprehensive Information Security Plan 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 Plan

The Information Security plan is a coherent set of information security policies, processes, systems, and objectives necessary for cost-effectively managing risks related to University information assets. It is the “blueprint” for how Information Security activities shall be conducted and refined.

3.8 Information Security Program

The Information Security program represents all interrelated services, activities, and initiatives needed to meet the security objectives defined within the Information Security Plan.

3.9 Information Processing Facilities
3.10 Information Asset

Information Assets are valued physical and electronic resources that can be used to create, store, distribute, use, integrate and manipulate information.

3.11 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.

3.12 Information Security Incident

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

3.13 Data Maintenance

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

3.14 Data Inquiry

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

3.15 ISO

“ISO” refers to the International Organization for Standardization.

3.16 GLBA

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

3.17 HIPAA

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

3.18 CFR

“CFR” refers to the Code of Federal Regulations.

3.19 PCI-DSS

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

4 Policy and Procedure Statements

4.1 Information Security Plan

Consistent with the roles and responsibilities outlined in this policy (4.3), Appalachian State University shall develop, implement, and maintain a comprehensive Information Security Plan. This plan 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 - Appalachian State University's Information Security Plan 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, Appalachian State 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 Information Security Plan 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 Information Security Advisory Council - To ensure the Information Security Plan is aligned to the University 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.

4.2.2 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.

4.2.3 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 Appalachian State 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 University Information Security policy.
2. Providing executive oversight and support of information security plan.
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 - The Chief Information Officer shall be responsible for:

1. Monitoring the effectiveness of the information security program.
2. Maintaining alignment of IT services with institutional risk tolerance levels.
3. Periodically reporting Information Security posture to the Chancellor and Chancellor’s Cabinet.

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 security program.
2. Facilitating information security governance and collaboration.
3. Advising 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.
3. Ensuring security liaisons are appointed for all reporting units (see below).

4.3.5 Information Security Liaisons - University Security Liaisons shall be responsible for:

1. Acting as central point of contact for security efforts and issues.
2. Periodically meeting with the ITS-OIS staff for awareness and updates.
3. Providing feedback to ITS-OIS staff on information security improvements.
4. Periodically reporting regarding unit’s security status and compliance with relevant policies and standards.
4.3.6 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 (see 4.4.3c).
2. Risk treatment options, including any cost-effective controls, will be analyzed and identified.
3. Appreciable 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 3.0-12.2

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 3.0-12.7
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 3.0-12.6
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. Reference: ISO 27002:2013-7.3, 8.1.4; HIPAA: 45 CFR § 164.308(a)(3)(ii)(C); PCI-DSS 3.0: 8.1.3; 9.3

4.4.3 Asset Management

1. Data Governance - All institutional data will be considered the property of Appalachian State 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 - 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 27002:2013-8.1.3,8.2.3
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)(i); HIPAA-45 CFR -§164.310(d)(2)(i),§164.310(d)(2)(ii), PCI-DSS 3.0-9.8

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:
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 3.0-8.1.2*

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 3.0-7.1*

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)*

7. **Source Code Control** - Access to program source code for University systems will be strictly controlled to authorized individuals only. *Reference: ISO 27002:2013-9.4.5*

### 4.4.5 Cryptographic Security

1. **Use of Cryptographic Controls** - University information systems will utilize cryptographic controls to address appreciable risks related to the confidentiality and integrity of sensitive information and non-repudiation of electronic transactions with University systems. *Reference: ISO 27002:2013-10.1.1; HIPAA-45 CFR §164.312(a)(2)(e); PCI-DSS 3.0-3.4*

2. **Key Management** - University cryptographic keys will be generated, stored, and managed in a secure and approved manner. *Reference: ISO 27002:2013-10.1.2; PCI-DSS 3.0-3.5,3.6*

### 4.4.6 Physical and Environmental Security

1. **Physical Security Perimeters** - Information processing facilities and other secure areas will have well defined physical boundaries and implement sufficient physical barriers and restrictions to prevent unauthorized entry and physical access. *Reference: ISO 27002:2013-11.1.1; HIPAA-45 CFR §164.310(a)(1); PCI-DSS 3.0-9.1.1,9.4*

2. **Physical Entry Controls** - Only authorized personnel will be allowed to enter information processing facilities and other secure areas. All access attempts will be monitored and logged. Unauthorized access attempts will be addressed. *Reference: ISO 27002:2013-11.1.2; HIPAA-45 CFR §164.310(a)(2); PCI-DSS 3.0-9.1.9.2*

3. **Environmental Threats** - Information processing facilities will be protected against natural disasters and damage from environmental accidents. *Reference: ISO 27002:2013-11.1.14*

4. **Information Processing Facilities** - Work conducted in Information Processing Facilities will adhere to all documented safety and security requirements. *Reference: ISO 27002:2013-11.1.5*


6. **Unattended Equipment** - Unattended user equipment will have appropriate protection controls and measures to prevent unauthorized use. *Reference: ISO 27002:2013-11.2.8; PCI-DSS 3.0-8.1.8*

### 4.4.7 Operations Security

1. **Change Management** - Changes to business processes, information processes, facilities, and systems that may impact University information security will be appropriately identified, evaluated, communicated, and controlled. *Reference: ISO 27002:2013-12.1.3; PCI-DSS 3.0-6.4*

2. **Capacity Management** - The utilization of high value information resources will be monitored, assessed, and optimized to maximize availability in conjunction with appropriate controls. *Reference: ISO 27002:2013-12.1.3*

3. **Separation of Development, Testing, and Operational Environments** - Development, testing, and operational environments will be sufficiently separated and any sensitive information stored in these environments will have at least equivalent protection measures. *Reference: ISO 27002:2013-12.1.4; PCI-DSS 3.0-6.4.1*

4. **Malware Protection** - Detection, Prevention, and Recovery measures will be established to protect University information systems against malicious software applications. *Reference: ISO 27002:2013-12.2; HIPAA-164.308(a)(5)(ii)(B); PCI-DSS 3.0-5.1*

5. **Information Backups** - Backup copies of valuable data will be regularly created, stored securely, validated, and periodically tested for recoverability. *Reference: ISO 27002:2013-12.3; GLBA-16 CFR 314.4(2); HIPAA-45 CFR §164.310(d)(2)(4); PCI-DSS 3.0-8.1.8*
6. Logging and Monitoring - Important events related to University information assets will be reliably archived, regularly reviewed, and protected from tampering and unauthorized access. Reference: ISO 27002:2013-2.4; HIPAA-45 CFR §164.312(b); PCI-DSS 3.0-10

7. Clock Synchronization - University information systems’ clocks will be synchronized against a single authorization reference time source. Reference: ISO 27002:2013-12.4.4; PCI-DSS 3.0

8. Vulnerability Management - Security weaknesses related to University information systems will be promptly identified, assessed, and remediated according to the associated risks they present to the University. Reference: ISO 27002:2013-12.6

9. Information System Audits - Audit activities involving verification of production information systems will be carefully planned, formally authorized, and executed by qualified personnel only. Reference: ISO 27002:2013-12.7

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, 13.1.2

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)

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)


5. Information Transfer - Transfer methods and controls will be defined and adhered to in order to protect University sensitive information traversing all forms of communication facilities to both internal and external senders and recipients. Reference: ISO 27002:2013-13.2.1; GLBA -16 CFR 314.4(2)

6. Electronic Messaging - Protection measures will be established to safeguard University electronic messaging solutions from unauthorized access, modification or denial of service. Retention of electronic messaging communication will be maintained in an approved manner. Reference: ISO 27002:2013-13.2.3

7. Confidentiality Agreements - Confidentiality agreements will be used to establish legally enforceable terms of utilization and access for University confidential information for both external parties and employees. Reference: ISO 27002:2013-13.2.4

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

4.4.10 Supplier Relationship

1. Supplier Security Agreements - Security requirements will be documented and agreed with each supplier that may access, process, store, or communicate University owned data. Reference: ISO 27002:2013 - 15.1.1, 15.1.2; GLBA -16 CFR 314(d1); 16 CFR 314(d2)

2. Monitoring and Review of Supplier Services - Periodic review of supplier services will be conducted to ensure that related security agreements are being adhered to and enforced. Reference: ISO 27002:2013-15.2.1

4.4.11 Information Security Incident Management

1. Reporting of Information Security Events - Information security events will be reported through an approved channel and
2. Reporting of Information Security Weaknesses - Employees and contractors will be encouraged to note and report any appreciable information security weaknesses observed in systems or services. \textit{Reference: ISO 27002:2013-16.1.3;}

3. Response to Information Security Incidents - Response actions related to security incidents will adhere to a documented set of procedures, including appropriate communication and coordination of efforts. \textit{Reference: ISO 27002:2013-16.1.4, 16.1.5; GLBA - 16 CFR 314.4(3)}

4. Learning From Information Security Incidents - Knowledge gained during the analysis of security incidents will be captured, reviewed, and appropriately shared to identify security corrections or control measures that may help address similar events. \textit{Reference: ISO 27002:2013-16.1.6}


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. \textit{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. \textit{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. \textit{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. \textit{Reference: ISO 27002:2013-18.1.2}

3. Protection of Records - University records will be protected from loss, destruction, falsification, and unauthorized release in accordance with legal, regulatory, and contractual business requirements. \textit{Reference: ISO 27002:2013-18.1.3}

4. 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. \textit{Reference: ISO 27002:2013-18.1.4}

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. \textit{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. \textit{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. \textit{Reference: ISO 27002:2013-18.2.3}

5 Additional References

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

6 Authority

\textit{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