Radford University
Information Technology Security Standard 5003s-01

IT Security Office

October 20, 2022

Preface

Date and Purpose

October 20, 2022 – Clarified IT Security Audits Requirements (2.7.2).

Notice

It is the reader's responsibility to ensure they have the latest version of this Standard. Revision questions should be directed to the University's Information Security Officer (ISO). The most recent, approved version of this Standard will always be available upon request and on the University's Information Technology Services (ITS) website. Both the Information Technology Advisory Committee (ITAC) and the it-info listserv will be notified when new revisions are approved and released for publication.

History

October 20, 2022 – Clarified IT Security Audits Requirements (2.7.2).
May 18, 2020 -- Removed reference to SEC501 (Base Standards), clarification on account lockouts (5.3.2), corrections to management of encryption keys (6.3.2) and removing requirement for digital signatures in email (8.5.2), and updated definition for sensitive systems.
February 21, 2019 – Clarified log review (9.3.2), clarified scope for annual DR testing (3.2.2), clarified baseline security configurations (4.3.2) and clarified wording for two-factor authentication (5.2.2).
September 1, 2018 - Updated Roles, including responsibilities around Third-Party Hosted Systems/Applications, (2.2.5), Application Administrator (2.2.8) and Training (8.3).
April 15, 2016 – updated sections 2.2.3, 4.3.2, and 4.7.2 to clarify annual vulnerability scanning requirements
January 13, 2015 – updated definitions for clarity; updated section for "Password Management" to reflect change to 180-day password expiration
March 18, 2013 – updated section "Exceptions to Security Requirements" to reflect proper approval process, and Requirements for "Account Management" to reflect changes in responsibility for access approvals
February 13, 2012 – Updated to reflect change in system idle timeout setting
February 9th, 2011 – Original Version 1 (5003s-01) developed, based on Commonwealth of Virginia ITRM Standard SEC501-01 (Revision 5)

Review Process

The Office of Audit and Advisory Services (OAAS) will provide the initial review of this Standard and all subsequent revisions. The Information Technology Advisory Committee (ITAC) will be notified of changes where appropriate.

Approval Authority

The University President, or designee, has approval authority over this Standard.

Publication Designation

Information Technology Security Standard

Publication Number

5003s-01

Purpose of This Standard

To define the minimum requirements for the University's Information Security Program.

General Responsibilities

The Chief Information Officer (CIO) has designated the Information Security Officer (ISO) to develop information security policies, procedures, and standards to protect the confidentiality, integrity, and availability of the University's information technology systems, networks and data. Therefore, the ISO is the author and maintainer of this Standard.

Subject Area

Information Technology Security

Effective Date

October 20, 2022

Compliance Date

October 20, 2022

Supersedes

None

Scheduled Review

One (1) year from effective date.

Authority

Memorandum of Understanding between Radford University and the Commonwealth of Virginia Section 23-38.90.

Scope

This Standard applies to all of Radford University.

Base Standards

1. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ISO/IEC 27000 series.
2. National Institute of Standards and Technology (NIST) Special Publication 800-88.

Related Policy

Current version of the University's Information Security Policy IT-PO-1503.

Contents

1 INTRODUCTION

1.1 Intent

The intent of this Standard is to establish a baseline for information security and risk management activities for all of Radford University. These baseline activities include, but are not limited to, any regulatory requirements that the University is subject to, information security best practices, and the requirements defined in this Standard. These information security and risk management activities will provide protection of, and mitigate risks to, University information systems, networks, and data.

This Standard defines the minimum acceptable level of information security and risk management activities for the University, commensurate with sensitivity and risk.

The University Information Security Program consists of the following major component areas:

1. Risk Management
2. IT Contingency Planning
3. Information Systems Security
4. Logical Access Control
5. Data Protection
6. Facilities Security
7. Personnel Security
8. Threat Management
9. IT Asset Management

Each component listed above contains requirements that, taken together, comprise the University's IT Security Standard. This Standard recognizes that University departments may procure IT equipment, systems, and services from third parties. In such instances, University departments remain accountable for maintaining compliance with this Standard and must enforce these compliance requirements through documented agreements with third-party providers and oversight of the services provided.

1.2 Organization of this Standard

The component areas of the University's Information Security Program provide the organizational framework for this Standard. Each component area consists of one or more sections containing:

1. A Purpose statement that provides a high-level description of the component area or subcomponent area and its importance.
2. Requirements that are mandatory technical and/or programmatic activities for a specific component area.
3. As appropriate, recommendations that are advisory in nature and provide guidance to departments in answering specific questions.
4. Notes, which provide rationale and explanation regarding the requirements.
5. Examples that describe the ways in which the requirements might be met.

1.3 Roles and Responsibilities

The University should utilize organizational charts depicting the reporting structure of employees when assigning specific responsibilities for the security of IT systems, networks, and data. The University shall maintain documentation regarding specific roles and responsibilities relating to information security.

1.4 Information Security Program

The University shall establish, document, implement, and maintain its information security program appropriate to its business and technology environment in compliance with this Standard. In addition, because resources that can reasonably be committed to protecting IT systems are limited, the University must implement its information security program in a manner commensurate with sensitivity and risk.

1.5 Exceptions to Security Requirements

If a University department determines that compliance with the provisions of this Standard or any related information security standard would adversely impact an official University business process, the University department may request approval to deviate from a specific requirement by submitting an exception request to the Chief Information Officer (CIO). For each exception, the requesting department shall fully document:

1. The business need and justification
2. The scope and extent of the deviation
3. Mitigating safeguards
4. The related risks
5. The specific duration
6. The department Dean or Director’s approval
7. Division Head’s signature accepting residual risks

Each request shall be in writing to the CIO using the IT Security Standard 5003s Exception Request located at: https://www.radford.edu/content/dam/departments/administrative/doit/documents/ITSecurityStandardExceptionVer1.pdf. The request must be approved by the department’s Dean or Director, and by the Division Head making the request indicating acceptance of and responsibility for the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and identified related risks. Requests for exception shall be evaluated and decided upon by the University’s Information Security Officer (ISO) and CIO. The requesting party will be informed of the decision. An exception cannot be processed unless identified related risks are clearly stated and the department’s Dean or Director, and the area Division Head has approved, indicating acceptance of and responsibility for these risks. In addition, when a requirement defined in this standard is not supported by features of the system, mitigating controls must be implemented to address the requirement.

1.6 Exemptions from this Standard

The following are explicitly exempt from complying with the requirements defined in this Standard:

1. Systems under development and/or experimental systems that do not create additional risk to production systems, networks, and data. To be considered for exemption, these systems must not contain Highly Sensitive data.
2. Surplus and retired systems.
3. Non-sensitive systems.

2 RISK MANAGEMENT

2.1 Purpose

Risk Management delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise IT systems, networks and data. This section defines requirements for the following areas:

1. Key Information Security Roles and Responsibilities
2. Business Impact Analysis
3. IT System and Data Sensitivity Classification
4. IT System Inventory and Definition
5. Risk Assessment
6. IT Security Audits

2.2 Key Information Security Roles and Responsibilities

2.2.1 Purpose

This Section defines the key IT security roles and responsibilities included in the Information Security Program. These roles and responsibilities are assigned to individuals and may differ from the role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

2.2.2 Chief Information Officer of the University (CIO)

At Radford University, the CIO is also the Associate Vice President for Information Technology and may be referred to as either in this Standard. The University President has delegated Information Technology duties and responsibilities to the CIO. As a part of these delegated duties and responsibilities, the CIO is responsible for the overall security of the University's information systems, networks, and data. The CIO's information security responsibilities include the following:

1. Designate an Information Security Officer (ISO) for the University. Note: The University should have at least one backup ISO.
2. Ensure that an information security program is maintained that is sufficient to protect the University's IT assets and is documented and effectively communicated to the University.
3. Ensure that a System Owner is identified for each University system. Each System Owner shall work with Data Owner(s), Data Custodian(s), and System Administrator(s) in the documentation, operation, and maintenance of the University IT system.
4. Review and approve the University's Business Impact Analysis (BIAs), Enterprise Risk Assessments (RA), and IT Disaster Recovery Strategy and Plans.
5. Provide the resources to enable University employees to carry out their responsibilities for securing IT systems, networks, and data.
6. Ensure compliance is maintained with IT Security Audit requirements. This compliance must include, but is not limited to:
   (a) Requiring development and implementation of a plan for IT security audits.
   (b) Requiring that the planned IT security audits are conducted.
   (c) Receiving reports of the results of IT security audits.
   (d) Requiring development of Corrective Action Plans to address findings of IT security audits.
7. Prevent conflict of interests and adhere to the concept of separation of duties by assigning roles so that:
   (a) The ISO is not a System Owner or a Data Owner except in the case of compliance systems for information security.
   (b) The System Owner and the Data Owner are not System Administrators for IT systems or data

they own.

(c) The ISO, System Owners, and Data Owners are all University employees.

8. Ensure that an information security awareness and training program is established.

2.2.3 Information Security Officer (ISO)

The ISO is responsible for developing, coordinating, and managing the University's information security program. The ISO's duties are as follows:

1. Develop and manage an information security program in a manner commensurate with risk.
2. Develop and manage an Intrusion Detection System (IDS) program in a manner commensurate with risk.
3. Develop and maintain an information security awareness and training program for University IT users per the *IT5103 Security Awareness Training Policy*.
4. Verify and validate that all University IT systems, networks and data are classified for sensitivity and risk and maintain awareness of the security status of IT systems.
5. Implement and maintain the appropriate balance of preventative, detective and corrective controls for University IT systems commensurate with data sensitivity, risk, and systems criticality.
6. Mitigate and report all IT security incidents in accordance with 2.2-5514 of the Code of Virginia and take appropriate actions to prevent recurrence.
7. Provide solutions, guidance, and expertise in IT security matters.
8. Review System Security Plans and require that the System Owner implement appropriate levels of security controls on the IT system to provide protections against security risks.
9. Perform annual internal reviews and vulnerability assessments for university-hosted sensitive systems.
10. Develop and lead the Computer Security Incident Response Team (CSIRT) to prepare for and respond to intrusions and threats.
11. Provide annual role-based training to System Owners, Data Owners, Data Custodians, System Administrators, and Application Administrators.

2.2.4 Privacy Officer

The University must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise, these responsibilities are carried out by the ISO. The Privacy Officer provides guidance on:

1. The requirements of state and federal privacy laws.
2. Disclosure of and access to Highly Sensitive data.
3. Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

2.2.5 System Owner

The System Owner is the University manager responsible for having an IT system documented, operated, and maintained. An IT System must have only one System Owner. With respect to IT security, the System Owner's responsibilities include the following:

1. Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
2. Ensure that system documentation and diagrams are updated with system changes.

3. Manage system risk and develop any additional information security policies and procedures required to protect the system in a manner commensurate with risk.
4. Maintain compliance with University Information Security policies and standards in all IT system activities for both systems hosted by a third-party provider and university-hosted systems.
5. Maintain compliance with the Third-Party Hosted System/Application Security Review Procedures when system is hosted by a third-party provider.
6. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.
7. Designate System Administrators, Data Owner, and Application Administrator for the system.
8. Complete annual role-based training.

Note: A System Owner can own multiple IT systems.

2.2.6 Data Owner

The Data Owner is the University manager responsible for the policy and practice decisions regarding University data, and is responsible for the following:

1. Evaluate and classify sensitivity of the data.
2. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.
3. Communicate data protection requirements to the System Owner.
4. Define requirements for access to the data.
5. Complete annual role-based training.
6. Approve access to data.
7. Appoint a Data Custodian, where appropriate.

Note: A Data Owner can own data on multiple IT systems. Data may have multiple data owners.

2.2.7 System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. Each system should have at least two System Administrators (one primary, one secondary). The System Administrator is responsible for the following:

1. Assist University management in the day-to-day administration of IT systems.
2. Implement security controls and other requirements of the University's information security program on IT systems for which the System Administrator has been assigned responsibility.
3. Monitor system logs for anomalous activity and notify IT Security Office of any potential threats or compromises of the system.
4. Ensure system and security updates are applied in a timely manner.
5. Complete annual, role-based training.

Note: System Administrators can assume responsibility for multiple IT systems but may not also be the System Owner or Data Owner.

2.2.8 Application Administrator

The Application Administrator is the University manager responsible for the operations and maintenance of the application, at the direction of the System Owner, Data Owner, and/or Data Custodian. Each system should have at least two Application Administrators (one primary, one secondary) where possible. The Application Administrator is responsible for the following:

1. Implement security baseline, controls, and other requirements of the University's information security program on IT applications for which the Application Administrator has been assigned responsibility.
2. If the application requires communication with other University systems, work with Information Technology Services to update or implement firewall rules and integrations with other systems.
3. Assign access and accounts, adhering to Section 5: Logical Access Control. Promptly remove access of users who no longer need access and maintain principle of least privilege.
4. Monitor application logs for anomalous activity and notify the IT Security Office of any potential threats or compromises of the application or accounts.
5. Ensure application and security updates are applied in a timely manner.
6. Complete annual role-based training.

2.2.9 Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

1. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.
2. Establish, monitor, and operate IT systems in a manner consistent with University Information Security policies and standards.
3. Provide Data Owners with reports, when necessary and applicable.
4. Complete annual role-based training.

2.2.10 IT System Users

All users of University IT systems are responsible for the following:

1. Read and comply with University information security program policies, procedures and standards.
2. Report breaches of IT security, actual or suspected, to University management and/or the ISO.
3. Take reasonable and prudent steps to protect the security of IT systems, networks, and data to which they have access.
4. Complete annual IT Security Awareness training as required in *IT5103 Security Awareness Training Policy*. Failure to complete annual IT Security Awareness training may result in account suspension.

Note: Other roles may be assigned to contractors working with University systems. For roles assigned to contractors, the contract language must include specific responsibility and background check requirements.

2.3 Business Impact Analysis

2.3.1 Purpose

Business Impact Analysis (BIA) delineates the steps necessary for the University to identify business functions that are essential to its mission and identify the resources that are required to support these essential business functions.

2.3.2 Requirements

The University should:

1. Require the participation of System Owners and Data Owners in the development of the University's BIA.
2. Identify business functions.
3. Identify essential business functions.

   Note: A business function is essential if disruption or degradation of the function prevents the University from performing its mission, as described in the University mission statement.
4. Identify dependent functions, if any. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.
5. For each essential business function and dependent function, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover an essential function or a dependent function shall be considered Business Impact Essential (BIA Essential). For each such system, the University shall:

   (a) Determine and document the required Recovery Time Objective (RTO), based on University goals and objectives.

   (b) Determine and document the Recovery Point Objectives (RPO).
6. Use the IT information documented in the BIA report as a primary input to Risk Assessments, IT Contingency Planning and IT System Security Plans.
7. Conduct periodic review and revision of the University BIA, as needed, but at least once every three years.

2.4 IT System and Data Sensitivity Classification

2.4.1 Purpose

IT System and Data Sensitivity Classification requirements identify the steps necessary to classify all IT systems, networks and data. See *Data and System Classifications Standard 5102s* for additional details.

Data Owners and System Owners must classify each IT system according to the requirements in Standard 5102s.

2.4.2 Requirements

The ISO shall:

1. Require that the Data Owner identify the type(s) of data handled by the University IT system.
2. Require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.
3. Require that the Data Owner determine the potential damages to the University of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system and classify the sensitivity of the data accordingly.
4. Review IT system and data classifications and subsequently obtain CIO approval of these classifications.
5. Verify and validate that all University IT systems, networks and data have been reviewed and classified for sensitivity.
6. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-

users.

7. Require that the University prohibit posting any data classified as Highly Sensitive or Protected on a public web site, FTP server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the CIO identifying the business case, risks, mitigating controls, and identified residual risks. This requirement may be implemented by policy, procedure and/or standards.
8. Use the information documented in the system and data classification as a primary input to the Risk Assessment process defined in this Standard.

2.5 IT System Inventory and Definition

2.5.1 Purpose

IT System Inventory and Definition requirements identify the steps in listing and marking the boundaries of IT systems in order to provide cost-effective, risk-based security protection for IT systems and for the University as a whole.

2.5.2 Requirements

The IT Security office shall provide a consulting role to the responsible parties to:

1. Document IT systems owned by the University, including system ownership and boundaries, and update the documentation as changes occur.
2. Maintain or require that its networking group/service provider maintain updated network diagrams.
3. Maintain a reference list that correlates each system with the components required to run the system (such as servers, networks, personnel, etc.).

2.6 Risk Assessment

2.6.1 Purpose

Risk Assessment (RA) requirements delineate the steps the University must take to:

1. Identify potential threats to an IT system and the environment in which it operates.
2. Determine the likelihood that threats will materialize.
3. Identify and evaluate vulnerabilities.
4. Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

Note: This Standard requires a risk assessment based on operational risk.

2.6.2 Requirements

For each IT system classified as sensitive or BIA Essential, the University shall:

1. Conduct and document a RA of the IT system due to material change, but not less than once every three years.
2. Conduct and document an annual self-assessment to determine the continued validity of the RA.
3. Prepare a report of each RA that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.

2.7 IT Security Audits

2.7.1 Purpose

IT Security Audit requirements define the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective.

2.7.2 Requirements

Using the identified list of IT systems classified as sensitive, the University shall

1. Determine the IT audit universe over which IT security audits will be conducted.
2. Categorize the IT audit universe into audit groups.
3. Require that, based on a risk assessment, IT security audits will be conducted on each audit group over a five-year period.
4. Assign the CIO or designee to manage the IT security audit requirements.

3 IT CONTINGENCY PLANNING

3.1 Purpose

IT Contingency Planning delineates the steps necessary to plan for and execute recovery and restoration of IT systems, networks and data if an event occurs that renders the IT systems, networks and/or data unavailable. This component of the University Information Security Program defines requirements in the following areas:

1. Continuity of Operations Planning.
2. Disaster Recovery Planning.
3. IT System and Data Backup and Restoration.

3.2 Continuity of Operations Planning

3.2.1 Purpose

The Continuity of Operations Plan (COOP) requirements are outside of the scope of this Standard. This section addresses only the IT disaster recovery components of the COOP for IT systems, networks, and data. These IT disaster recovery components of the COOP identify the steps necessary to provide continuity for essential University IT systems, networks, and data.

3.2.2 Requirements

The University shall:

1. Designate an employee to collaborate with the University Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery (DR) planning activities. Unless otherwise specified, the ISO assumes this designation.
2. Based on BIA and RA results, develop IT disaster components of the University COOP which identifies:
   (a) Each IT system that is necessary to recover essential business functions or dependent business

functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each.

(b) Personnel contact information and incident notification procedures.

(c) The necessary components to recover each identified system.

Note: If the COOP contains confidential information, those components should be protected, and a backup stored at a secure off-site location.

3. Require a DR exercise of BIA Essential systems to assess their adequacy and effectiveness at least every three years.
4. Require review and revision of IT DR components following the exercise (and at other times as necessary).

3.3 IT Disaster Recovery Planning

3.3.1 Purpose

IT Disaster Recovery Planning is the component of Continuity of Operations Planning that identifies the steps necessary to provide for restoring essential business functions on a schedule that supports the University's mission. These steps lead to the creation of an overall IT Disaster Recovery Strategy (DRS).

3.3.2 Requirements

The University shall:

1. Develop and maintain an IT DRS, which supports the restoration of essential business functions and dependent business functions.
2. Require approval of the IT DRS by the CIO.
3. Require annual reviews, reassessments, testing, and revisions of the IT DRS to reflect changes in essential business functions, services, IT system hardware and software, and personnel.
4. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.

3.4 IT System and Data Backup and Restoration

3.4.1 Purpose

IT System and Data Backup and Restoration requirements identify the steps necessary to protect the availability and integrity of University data documented in backup and restoration plans.

3.4.2 Requirements

The University shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, networks, data and applications in accordance with University requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media.
2. Store off-site backup media in an off-site location that is geographically separate and distinct from the primary location.
3. Performance of backups only by authorized personnel.
4. Review of backup logs after the completion of each backup job to verify successful completion
5. Approval of backup schedules of a system by the System Owner in consultation with the Data Owner.

6. Approval of emergency backup and operations restoration plans by the System Owner.
7. Protection of any backup media that is sent off-site (physically or electronically) or shipped by the United States Postal Service or any commercial carrier, in accordance with University requirements.
8. Authorization and logging of deposits and withdrawals of all media that is stored offsite.
9. Retention of the data handled by an IT system in accordance with the Commonwealth of Virginia or the University's records retention policy.
10. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.
11. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.
12. For BIA Essential systems, document and exercise a strategy for testing backup and recovery procedures, in accordance with the University's Continuity of Operations Plan, at least every three years.

4 INFORMATION SYSTEMS SECURITY

4.1 Purpose

Information Systems Security requirements delineate steps to protect information systems in the following areas:

1. IT System Security Plans
2. IT System Hardening
3. IT Systems Interoperability Security
4. Malicious Code Protection
5. Systems Development Life Cycle Security
6. Application Security
7. Wireless Security

4.2 IT System Security Plans

4.2.1 Purpose

IT System Security Plans (SSP) document the security controls required to demonstrate adequate protection of information systems against security risks including those risks identified in risk assessments.

4.2.2 Requirements

Each System Owner of a sensitive or BIA Essential IT system shall:

1. Document an IT System Security Plan (SSP) for the IT system based on the results of the risk assessment. This documentation shall include a description of:
   (a) All existing and planned security controls for the IT system, including a schedule for implementing planned controls.
   (b) How these controls provide adequate mitigation of risks to which the IT system is subject.

2. Submit the IT System Security Plan to the ISO for review.
3. Update the IT System Security Plan every three years, or more often if necessary (e.g., due to material change), and resubmit to the ISO.

4.3 IT System Hardening

4.3.1 Purpose

IT System Hardening requirements delineate technical security controls to protect IT systems against security vulnerabilities.

4.3.2 Requirements

The University shall or shall require that its service provider:

1. Identify, document, and apply appropriate baseline security configurations to all University IT systems.

   Note: The University may develop University specific baseline security configuration standards or may elect to use baseline security configuration standards that are publicly available, such as those developed by the Center for Internet Security (www.cisecurity.org).
2. Maintain records that document the application of baseline security configurations.
3. Monitor systems for security baselines and policy compliance.
4. Review and revise all baseline security configuration standards annually, or more frequently, as needed.

   Note: The University should establish a process to review applicable security notifications issued by equipment manufacturers, bulletin boards, security-related web sites, and other security venues, and establish a process to update security baseline configuration standards based on those notifications.
5. Reapply all baseline security configurations to University IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
6. Require annual operating system level vulnerability scanning of sensitive IT systems.
7. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.
8. Security patches should be applied when they can eliminate or mitigate applicable security vulnerabilities. The risks associated with applying security patches should be taken into consideration and compared against the risks of the identified security vulnerability. If no security patch is available, or is available but unable to be applied because doing so is deemed to be the greater risk, the following compensating controls may be utilized:
   (a) Modify or create access restrictions, e.g. firewalls, to limit access to the system.
   (b) Disable services or functionality related to the identified security vulnerability.
   (c) Raise awareness of the identified security vulnerability.
   (d) Increase IDS logging to detect potential attacks.

4.4 IT Systems Interoperability Security

4.4.1 Purpose

IT System Interoperability Security requirements identify steps to protect data shared with other IT systems.

4.4.2 Requirements

For every sensitive University IT system that shares data with non-University entities, the University shall require or shall specify that its service provider require:

Note: Best practice dictates that Interoperability Agreements should be in place for sensitive IT system interoperability between University departments. However, this Standard currently only requires agreements between University and non-University entities.

1. The System Owners, in consultation with the Data Owners, shall document IT systems with which data is shared. This documentation must include:
   (a) The types of shared data.
   (b) The direction(s) of data flow.
   (c) Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.
2. The System Owners of the IT systems which share data shall develop a written agreement that delineates security requirements for each interconnected IT system and for each type of data shared.
3. The System Owners of the IT systems that share data shall inform one another regarding other IT systems with which their IT systems interconnect or share data and shall inform one another prior to establishing any additional interconnections or data sharing.
4. The written agreement shall specify if and how the shared data will be stored on each IT system.
5. The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (e.g., FERPA, HIPAA, PCI, etc.) regarding handling, protection, and disclosure of the shared data.
6. The written agreement shall specify each Data Owner's authority to approve access to the shared data.
7. The System Owners shall approve and enforce the agreement.

4.5 Malicious Code Protection

4.5.1 Purpose

Malicious Code Protection requirements identify controls to protect IT systems from damage caused by malicious code.

4.5.2 Requirements

The University shall, or shall require that its service provider:

1. Prohibit all IT system users from developing or experimenting with malicious programs (e.g., viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.) unless this development or experimentation is for academic or research purposes in an offline environment that does not impact production systems, networks, or data.

2. Provide malicious program detection, protection, eradication, logging, and reporting capabilities.
3. Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.

   Example: The University may elect to provide protection against malicious code transmitted via email on the email servers and on the desktop.
4. Provide protection against malicious programs through the use of mechanisms that:
   (a) Eliminates or quarantines malicious programs that it detects.
   (b) Provides an alert notification.
   (c) Automatically runs scans on memory and storage devices.
   (d) Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device.
   (e) Allows only authorized personnel to modify program settings.
   (f) Maintains a log of protection activities.
5. Provide the ability to eliminate or quarantine malicious programs in email messages and file attachments as they attempt to enter the University's internal email system.
6. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.
7. Require all forms of malicious code protection to start automatically upon system boot.
8. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.
9. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shutdown, restoration, notification, and reporting requirements.
10. Require use of only new media (e.g., USB sticks, CD-ROM) or sanitized media for making copies of software for distribution.
11. Prohibit the use of shared computers and desktops (e.g., training rooms) to create distribution media.

4.6 Systems Development Life Cycle Security

4.6.1 Purpose

Systems Development Life Cycle (SDLC) security requirements document the security related activities that must occur in each phase of the development life cycle (from project definition through disposal) for University IT application systems.

4.6.2 Requirements

The University shall:

1. Incorporate security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.

Project Initiation

1. Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.
2. Classify the types of data that the system will process and the sensitivity of the proposed IT system.

3. Assess the need for collection and maintenance of Highly Sensitive data before incorporating such collection and maintenance in IT system requirements.
4. Develop an initial IT System Security Plan (see IT System Security Plans) that documents the security controls that the system will enforce to provide adequate protection against security risks.

Project Definition

1. Identify, develop, and document security requirements for the system during the Project Definition phase.
2. Incorporate security requirements in IT system design specifications.
3. Verify that the system development process designs, develops, and implements security controls that meet information security requirements in the design specifications.
4. Update the initial IT System Security Plan to document the security controls included in the design of the system to provide adequate protection against security risks.
5. Develop evaluation procedures to validate that security controls developed for a new system are working properly and are effective.

   Note: Some security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until after deployment of the system.

Implementation

1. Execute the evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

   Note: Results should be documented in a report, including identification of controls that did not meet design specifications.
2. Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the system.
3. Require that the system comply with all relevant Risk Management requirements in this Standard.
4. Update the IT System Security Plan to document the security controls included in the system as implemented to provide adequate protection against information security risks and comply with the other requirements (see IT System Security Plans) of this document.

Disposition

1. Require retention of the data handled by a system takes place in accordance with the Commonwealth of Virginia or the University's records retention policy prior to disposing of the system.
2. Require that electronic media is sanitized prior to disposal so that all data is removed from the system.
3. Verify the disposal of hardware and software in accordance with the *Data Storage and Media Protection Policy 5102*.

4.7 Application Security

4.7.1 Purpose

Application security requirements define the high-level specifications for securely developing and deploying University applications.

4.7.2 Requirements

The University ISO is accountable for ensuring the following steps are documented and followed:

Application Planning

1. Data Classification - Data used, processed, or stored by the proposed application shall be classified as defined in Standard 5102s.
2. System Classification – Systems shall be classified as Sensitive or Non-Sensitive as defined in Standard 5102s.
3. Risk Assessment - A risk assessment shall be conducted for sensitive systems before development begins and after planning is complete.
4. Security Requirements -Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.
5. Security Design - Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store Highly Sensitive data in an application, the following design criteria must be addressed:
   (a) Encrypted communication channels shall be established for the transmission of Highly Sensitive data.
   (b) Highly Sensitive data shall not be visibly transmitted between the client and the application.
   (c) Highly Sensitive data shall not be stored in hidden fields that are part of the application interface.

Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.

1. Authentication -Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.
2. Session Management -Any user sessions created by an application shall support an automatic inactivity timeout function.
3. Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures).

   Note: The University may consider the use of data scrubbing routines to remove all Highly Sensitive data from non-production data storage.
4. Input Validation -All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.
5. Default Deny -Application access control shall implement a default deny policy, with access explicitly granted.
6. Principle of Least Privilege -All processing shall be performed with the least set of privileges required.
7. Quality Assurance -Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.

   Note: Source code auditing techniques include, but are not limited to:
   (a) Manual code review can identify vulnerabilities as well as functional flaws, but most University departments do not have the skilled security resources or time available within the software life cycle that a manual code review requires, and therefore, many who decide to perform manual code reviews can only analyze a small portion of their applications
   (b) Application penetration testing tries to identify vulnerabilities in software by launching as many known attack techniques as possible on likely access points in an attempt to bring down the application or the entire system

(c) Automated source code analysis tools make the process of manual code review more efficient, affordable, and achievable. This technique of code audit results in significant reduction of analysis time, actionable metrics, significant cost savings, and can be integrated into all points of the development life cycle.

8. Configure applications to clear the cached data and temporary files upon exit of the application or log off of the system.

Production and Maintenance

1. Production applications shall be hosted on servers compliant with the University Security requirements for IT system hardening.
2. Applications for sensitive systems shall have vulnerability scans run against the applications and supporting server infrastructure at least annually, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.

4.8 Wireless Security

4.8.1 Purpose

Wireless security requirements define the high-level specifications for the secure deployment and use of wireless networking.

4.8.2 Requirements

The University ISO is accountable for ensuring the following steps are followed and documented:

Wireless LAN (WLAN) Connectivity on the University networks

1. The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal University network.
   (a) WLAN infrastructure must authenticate client devices prior to permitting access to the WLAN.
   (b) User authorization infrastructure (e.g., Active Directory) must be used to authorize access to University resources.
   (c) Encryption must be used to access Highly Sensitive data (e.g. via VPN).
   (d) Physical or logical separation between WLAN and wired LAN segments must exist.
   (e) University WLAN access and WLAN egress traffic will be monitored for malicious activity, and associated event log files stored on a centralized storage device.

WLAN Hotspot (Wireless Internet)

1. When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:
   (a) WLAN Hotspots must have logical or physical separation from the University's LAN.
   (b) WLAN Hotspot access and WLAN egress traffic will be monitored for malicious activity, and log files stored on a centralized storage device.

Wireless Bridging

1. The following network configuration shall be used when bridging two wired LANs:
   (a) All wireless bridge communications must utilize secure encryption.
   (b) Wireless bridging devices must not be configured for any other service than bridging (e.g., a wireless access point).

5 LOGICAL ACCESS CONTROL

5.1 Purpose

Logical Access Control requirements delineate the steps necessary to protect IT systems, networks and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems, networks and data they are attempting to access. Users are accountable for any activity on the system and network performed with the use of their account. This component of the University Information Security Program defines requirements in the following three areas:

1. Account Management
2. Password Management
3. Remote Access

5.2 Account Management

5.2.1 Purpose

Account Management requirements identify those steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. The University should apply these Account Management practices to accounts on IT systems, including accounts used by vendors and third parties.

The requirements below distinguish between internal and external IT systems. Internal IT systems are designed and intended for use only by University employees, contractors, and business partners. External IT systems are designed and intended for use by University customers and by members of the public.

5.2.2 Requirements

The University shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

Note: It is strongly recommended technical controls be implemented wherever possible to fulfill the following requirements, understanding that manual processes must sometimes be implemented to compensate for technical controls that might not be feasible.

For all internal and external IT systems

1. Grant IT system users' access to IT systems, networks and data based on the principle of least privilege.
2. Define authentication and authorization requirements.
3. Establish policies and procedures for approving and terminating authorization to IT systems.
4. Require requests for and approvals of emergency or temporary access that:
   (a) Are documented according to standard practice and maintained on file.
   (b) Include access attributes for the account.
   (c) Are approved by the System Owner.
   (d) Expire after a predetermined period, based on sensitivity and risk.

5. Implement two-factor authentication, where possible, for access to IT systems.
6. System Owners and Data Owners must review all user accounts with elevated access privileges for the user's continued need to access sensitive systems. These reviews should be conducted and documented annually.
7. Notify Information Technology Services (ITS) when IT system user accounts are no longer required, or when a user's access level requirements change.
8. If the IT system is classified as sensitive, prohibit the use of guest (non-authenticated) accounts.
9. Prohibit the display of the last log on user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement.
10. Lock an account or automatically expire passwords if the account is not used for 180 days.
11. Disable unneeded accounts. Example: Root accounts that are not routinely used should be disabled.
12. Retain unneeded accounts in a disabled state in accordance with the Commonwealth of Virginia or the University's records retention policy.
13. Associate access levels with group membership, where practical, and require that every system user account be a member of at least one user group.
14. Require that the System Owner and the System Administrator investigate unusual system access activities.
15. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
16. Prohibit the granting of local administrator rights to users without documented need. Local administrative accounts are prohibited in areas subject to high risk or subject to additional regulations or standards (PCI, HIPAA, etc.).
17. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

For all internal IT systems

1. Require a documented request and approval by the user's supervisor and by the system's Data Owner or designee to establish an account on any sensitive IT system where the user will access or manage data other than their own.
2. Require a documented request and approval by the user's supervisor and approval by the System Owner or designee to establish an elevated or privileged account on any sensitive IT system.
3. Complete any University required background checks before establishing accounts, or as soon as practical thereafter.
4. Require secure delivery of access credentials to the user based on information already on file.
5. University departments must notify Human Resources and Information Technology Services (ITS) in a timely manner about termination or transfer of users with access rights to sensitive IT systems, networks, and data.
6. Promptly remove access when no longer required.

For all external IT systems

1. Require secure delivery of access credentials to users of all external IT systems.
2. Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of all sensitive external IT systems.
3. Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel.

For all service and hardware accounts

1. Document account management practices for all University created service accounts, including, but not limited to granting, administering, and terminating accounts.

5.3 Password Management

5.3.1 Purpose

Password Management specifies requirements for password use, storage and transmission to protect University IT systems, networks and data.

5.3.2 Requirements

The University shall or shall require that its service provider implement password management practices. At a minimum, these practices shall include the following components:

1. Users are responsible for selecting a unique password that is different from any other RU or non-RU system. As an example, users must not use the same password for Facebook and Banner.
2. Shared accounts that are used primarily for departmental or club activities may not be used to access sensitive systems.
3. Require passwords, PINs, or other modes of protection (e.g. pattern unlocking or fingerprints) on mobile devices such as smart phones, tablets, and laptops If using a PIN, it must have a minimum of 4 digits.
4. Require password complexity:
   (a) At least eight characters in length.
   (b) Password cannot contain the user's first name, last name, or account username.
   (c) Utilize at least three of the following four-character sets:
      i. Special characters (.@?)
      ii. Uppercase alphabetical characters (ABC)
      iii. Lowercase alphabetical characters (abc)
      iv. Numerical characters (123)

   Note: It is considered best practice not to base passwords on a single dictionary word and not to use words with numbers (or special characters) appended to the end. For example, "Classof2014!" would be an extremely weak password.
5. Require that default passwords be changed immediately after installation.
6. Prohibit the transmission of password data without the use of industry accepted encryption standards.
7. Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.
8. Require all sensitive IT system user accounts to change passwords at least every 180 days.
9. Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.
10. Where system configuration allows, configure all sensitive IT systems to maintain at least the last 6 passwords used in the password history files to prevent the reuse of the same or similar passwords.
11. Provide a unique initial password for each new account of sensitive IT systems and require that IT system users change the initial passwords issued upon first login.
12. For sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential

manner.

13. Prohibit the storage of passwords in clear text and, use the strongest available hashing storage solution to better withstand off-line attacks. The ISO should approve password hash storage solutions.

    Example: In a Microsoft Windows Active Directory domain that no longer has legacy clients, consider disabling LanMan hashing and require NT Hashing for password storage. In an OpenLDAP directory, use Secure SHA1 hashing (SSHA) rather than simple SHA1 hashing for password storage, etc.

    Note: System Owners should consult with the ISO to determine the strongest hash storage solution for their systems.
14. Limit access to files containing passwords to the IT system and its administrators, and log such access to these files.
15. Suppress the display of passwords on the screen as they are entered.
16. Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for University owned devices in non-academic areas.
17. Require passwords to be set on device management interfaces for all network devices.
18. Document and store hardware passwords securely.
19. Implement procedures to handle lost or compromised passwords and/or tokens.
20. In areas identified to be subject to specific regulations or standards, set an account lockout threshold of not greater than fifty (50) invalid attempts and the lockout duration for at least 15 minutes or set other mitigating controls.
21. User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by that user.

5.4 Remote Access

5.4.1 Purpose

Remote Access requirements identify the steps necessary to provide for the secure use of remote access to resources used by the University.

5.4.2 Requirements

The University shall or shall require that its service provider:

1. Commensurate with risk, protect the security of all remote access to the University’s sensitive IT systems, networks, and data by means of encryption, in a manner consistent with Section 6.3.

   Note: This encryption requirement applies both to session initiation (e.g., identification and authentication) and to all exchanges containing Highly Sensitive or Protected data.
2. Protect the security of remote file transfer of Highly Sensitive or Protected data to and from University IT systems by means of encryption, in a manner consistent with Section 6.3.
3. Require that IT system users obtain authorization and a unique user ID and password prior to using the University’s remote access capabilities.
4. Document requirements for the physical and logical hardening of remote access devices.
5. Require maintenance of auditable records of all remote access.
6. Where supported by features of the system, session timeouts shall be implemented after a period of no longer than 2 hours of inactivity, commensurate with sensitivity and risk.

6 DATA PROTECTION

6.1 Purpose

Data Protection requirements delineate the steps necessary to protect University data from improper or unauthorized disclosure. This component of the University Information Security Program defines requirements in the following two areas:

1. Data Storage Media Protection
2. Encryption

6.2 Data Storage Media Protection

6.2.1 Purpose

Data Storage Media Protection requirements identify the steps necessary for the appropriate handling of stored data to protect the data from compromise.

6.2.2 Requirements

The University shall or shall require that its service provider implement Data Storage Media Protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored Highly Sensitive or Protected data as the responsibility of the Data Owner.
2. Prohibit the storage of Highly Sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the CIO accepting identified residual risks. The exception shall include the following elements:
   (a) The business or technical justification.
   (b) The scope, including quantification and duration (not to exceed one year).
   (c) A description of all associated risks.
   (d) Identification of controls to mitigate the risks, one of which must be encryption.
   (e) Identification of any residual risks.

   Note: Non-network storage device or media, includes removable data storage media and the fixed disk drives of all desktops, mobile devices, and mobile storage devices.
3. Require logical and physical protection for all data storage media containing Highly Sensitive data, commensurate with sensitivity and risk.
4. Restrict the pickup, receipt, transfer, and delivery of all data storage media containing Highly Sensitive data to authorized personnel.
5. Procedures must be implemented and documented to safeguard handling of all backup media containing Highly Sensitive data. Encryption of backup media shall be considered where the data is classified as Highly Sensitive. Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.
6. Implement processes to sanitize data storage media prior to disposal or reuse.

6.3 Encryption

6.3.1 Purpose

Encryption requirements provide a framework for selecting and implementing encryption controls to protect Highly Sensitive data. See Data Breach Notification for notification requirements regarding a breach of unencrypted Highly Sensitive data.

6.3.2 Requirements

Commensurate with sensitivity and risk, the University or their service provider shall:

1. Define and document practices for selecting and deploying encryption technologies and for the encryption of data.
2. Document appropriate processes before implementing encryption. These processes must include the following components:
    a. A secure key management system for the administration and distribution of encryption keys.
    b. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.
    c. Response procedures in the event that encryption keys are compromised.
3. Require encryption for the transmission of Highly Sensitive data,

6.4 Protection of Sensitive Information on Non-Electronic Media

6.4.1 Purpose

This section outlines the best practice steps that should be taken to protect Highly Sensitive data that may be stored or transmitted on non-electronic media such as, the spoken word, paper documents, white or black boards, photographs, etc.

6.4.2 Recommendations

These recommendations apply to non-electronic media:

1. While in use, limit access based on a need to know basis by physically controlling access.

   For example, Highly Sensitive documents printed to a global printer should be retrieved without delay.
2. While not in use, store in a secure location with appropriate physical controls.
3. When no longer needed, securely destroy using appropriate destruction methods such as erasing white or black boards and shredding paper documents.

7 FACILITIES SECURITY

7.1 Purpose

Facilities Security requirements identify the steps necessary to safeguard the physical facilities that house IT equipment, systems, services, networks and personnel.

7.2 Requirements

The University shall or shall require that its service provider document and implement facilities security practices. At a minimum, these practices must include the following components:

1. Safeguard IT systems, networks and data residing in buildings, mobile facilities, and portable facilities.
2. Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.
3. Require appropriate environmental controls such as electric power, heating, fire suppression, humidity control, ventilation, air-conditioning and air purification, as required by the IT systems, networks and/or data.
4. Protect against unauthorized physical access.
5. Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege in all new installations.
6. Provide a system of monitoring and auditing physical access to sensitive IT systems.
7. Require that the ISO or designee annually review the list of persons allowed physical access to sensitive IT systems.
8. Should unauthorized physical access occur, departments must alert the ISO as soon as practical.

8 PERSONNEL SECURITY

8.1 Purpose

Personnel Security requirements delineate the steps necessary to restrict access to IT systems, networks and data to those individuals who require such access as part of their job duties and responsibilities. This component of the University Information Security Program defines requirements in the following areas:

1. Access Determination and Control
2. Information Security Awareness and Training
3. Acceptable Use
4. Email Communications

8.2 Access Determination and Control

8.2.1 Purpose

Access Determination and Control requirements identify the steps necessary to restrict access to IT systems, networks, and data to authorized individuals.

8.2.2 Requirements

The University shall or shall require that its service provider document and implement access determination and control practices for all sensitive systems. At a minimum, these practices shall include the following components:

1. Perform background investigations of all internal IT System users in accordance with University HR background check policy. Existing users may be grandfathered under the policy and may not be required to have background investigations.

2. Restrict visitor access to facility areas that house sensitive IT systems, networks, or data.
3. Require non-disclosure and security agreements for access to IT systems, networks, and data.
4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist.
5. Establish termination and transfer practices that require return of logical and physical assets that provide access to sensitive IT systems, networks, and data and the facilities that house them.
6. Temporarily disable physical and logical access rights when personnel do not need such access for a prolonged period in excess of 30 days because they are not working due to leave, disability, or other authorized purpose, based on requests from departments.
7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes, based on requests from departments.
8. Establish separation of duties in order to protect sensitive IT systems, networks, and data, or establish compensating controls when constraints or limitations of the University prohibit a complete separation of duties.

   Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, routine monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.
9. Explicitly grant physical and logical access to sensitive IT systems, networks and, data and the facilities that house them based on the principle of least privilege.

8.3 Information Security Awareness and Training

8.3.1 Purpose

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems, networks, and data.

8.3.2 Requirements

The University ISO shall:

1. Include any University specific information security training requirements in the University information security awareness and training program.

   Example: A University department that processes data covered by the Health Insurance Portability and Accountability Act (HIPAA) or the Payment Card Industry Data Security Standard (PCI-DSS) must have an information security awareness training program that addresses specific data security requirements.
2. Require that all employees and contractors with access to sensitive systems receive information security awareness training during the University's training cycle.
3. Require additional role-based information security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.

   Example: The University employees and contractors who are members of the Disaster Recovery Team or Computer Security Incident Response Team require specialized training in these duties.
4. Monitor and track completion of information security training.
5. Require information security training before (or as soon as practicable after) IT system users receive access rights to the University's sensitive IT systems, and in order to maintain these access rights.

6. Develop an information security training program for end users that covers such topics as, but not limited to:
   (a) The University's policy for protecting IT systems, networks, and data, with a particular emphasis on sensitive IT systems, networks, and data
   (b) Proper use of data storage media
   (c) Proper use of encryption
   (d) Access controls, including creating and changing passwords and the need to keep them confidential
   (e) Acceptable use policies
   (f) Responsibility for the security of University data
   (g) Phishing
   (h) Social engineering
7. Develop an information security training program for System Owners, Data Owners, Data Custodians, System Administrators, and Application Administrators to cover such topics as, but not limited to:
   a. The concept of separation of duties
   b. Prevention and detection of information security incidents, including those caused by malicious code
   c. Roles and responsibilities
   d. System and Data Classification requirements
   e. Third Party Hosted system requirements
   f. System documentation requirements
8. Require documentation of IT system users' acceptance of the University's security policies after receiving information security training.

8.4 Acceptable Use

8.4.1 Purpose

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of University IT systems, networks and data.

8.4.2 Requirements

The University shall:

1. Document an acceptable use policy.
2. Direct the proper use of encryption for transmitting Highly Sensitive data.
3. Direct the use of an authorized University warning banner to communicate that IT systems and their use may be monitored and viewed by authorized personnel; and there is no expectation of privacy when using a University owned system or network.
4. Require acknowledgment that monitoring of IT systems, networks, and data may include, but will not be limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the University President or CIO); and user commands; email and Internet usage; and message and data content.
5. Prohibit users from:
   (a) Installing or using proprietary encryption hardware/software on University systems

(b) Tampering with security controls configured on University owned systems

(c) Installing unauthorized, personal software on University owned systems

(d) Adding system hardware to, removing system hardware from, or modifying system hardware on a University owned system

6. Prohibit the unauthorized storage, use, or transmission of copyrighted and licensed materials on University systems and networks.
7. Require documentation of IT system users' acceptance of the University's Acceptable Use Policy before, or as soon as practical after, gaining access to University IT systems.

8.5 Email Communications

8.5.1 Purpose

Email communications requirements identify the general steps to protect data stored and transmitted in email. University emails are legally discoverable and may be public records subject to a request under the Privacy Act of 1974 (as amended or the Freedom of Information Act [FOIA]).

8.5.2 Requirements

The University shall:

1. Require approved encryption technologies for the transmission of email and attached data that is classified as Highly Sensitive. Email must not be used to send Highly Sensitive data unless said data is encrypted.

   Note: Approved encryption technologies for email are OpenPGP or S/MIME based encryption.
2. Inform users that emails sent from University systems are public records of the Commonwealth of Virginia and must be managed as such. Email disclaimers, a set of statements either pre-pended or appended to emails, are frequently used to create awareness of how to treat the data in the email. However, an email disclaimer is not a substitute for judgment on what content to put into an email.

9 THREAT MANAGEMENT

9.1 Purpose

Threat Management delineates the steps necessary to protect IT systems, networks, and data by preparing for and responding to information security incidents. This component area of the Standard defines requirements for the following:

1. Threat Detection
2. Information Security Monitoring and Logging
3. Information Security Incident Handling
4. Data Breach Notification

9.2 Threat Detection

9.2.1 Purpose

Threat Detection requirements identify the practices for implementing intrusion detection and prevention.

9.2.2 Requirements

The University shall or shall require that its service provider implement threat detection practices that at a minimum include the following:

1. Designate an individual responsible for the University's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance. Unless otherwise specified, the ISO assumes this designation.
2. Implement an Intrusion Detection System (IDS).
3. Conduct IDS log reviews to detect new attack patterns as quickly as possible.
4. Develop and implement required mitigation measures based on the results of IDS log reviews.
5. Maintain regular communication with security research and coordination organizations, such as US CERT, REN-ISAC, etc., to obtain information about new attack types, vulnerabilities, and mitigation measures.

9.3 Information Security Monitoring and Logging

9.3.1 Purpose

Information Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity.

9.3.2 Requirements

The University shall, or shall require that its service provider, implement information security monitoring and logging practices that include the following components, at a minimum:

1. Designate individuals responsible for the development and implementation of information security logging capabilities.
2. Develop procedures for reviewing and administering the logs.
3. Enable logging on all sensitive IT systems. At a minimum, logs will include:
   (a) The event.
   (b) The user ID associated with the event.
   (c) The date and time the event occurred.
4. Monitor IT system logs, correlate information with other automated tools, identify suspicious activities, and provide alert notifications in compliance with *IT5200, Log Review and Storage Policy.*
5. Document standards that specify the type of actions an IT system administrator should take when a suspicious or apparent malicious activity is taking place.

   Example: Possible actions include stopping the event, shutting down the IT system, and alerting appropriate staff.

   Note: Multiple actions may be warranted and advisable, based on sensitivity and risk.

6. Prohibit the installation or use of unauthorized monitoring devices.
7. Prohibit the use of keystroke logging, except when required for security investigations and/or academic instruction/research purposes.

Note: For investigative purposes, the ISO has the responsibility to authorize monitoring or scanning activities for network traffic; application and information access; user commands; email and Internet usage; and message and information content for IT systems, networks and data.

9.4 Information Security Incident Handling

9.4.1 Purpose

Information Security Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to information security safeguards.

9.4.2 Requirements

The University shall document information security incident handling practices and, where appropriate, the University shall incorporate its service provider's procedures for incident handling practices that include the following, at a minimum:

1. Designate a Computer Security Incident Response Team (CSIRT) that includes personnel with appropriate expertise for responding to attacks.
2. Identify controls to deter and defend against attacks to best minimize loss or theft of information and disruption of services.
3. Implement proactive measures to defend against new forms of attacks and zero-day exploits.
4. Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems, networks and data.
5. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems.
6. Establish a process for reporting information security incidents to the ISO. All University departments must report information security incidents to the ISO.
7. Establish requirements for internal University information security incident recording and reporting requirements, including a template for the incident report.
8. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.

Note: The ISO, in conjunction with the CIO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any University-owned IT resource suspected to be the object of inappropriate use or violation of laws, regulations, policies, or standards in order to preserve evidence.

9.5 Data Breach Notification

9.5.1 Purpose

To specify the notification requirements for unauthorized release of unencrypted Highly Sensitive information.

9.5.2 Requirements

Should a data breach occur, the University shall:

1. Comply with Commonwealth of Virginia data breach notification laws (and any other applicable laws) in consultation with legal counsel as necessary.

10 IT ASSET MANAGEMENT

10.1 Purpose

IT Asset Management delineates the steps necessary to protect IT systems, networks and data by managing the IT assets themselves in a planned, organized, and secure fashion. This component area defines requirements for the following:

1. IT Asset Control
2. Software License Management
3. Configuration Management and Change Control

10.2 IT Asset Control

10.2.1 Purpose

IT Asset Control requirements identify the steps necessary to control and collect information about IT assets.

10.2.2 Requirements

Commensurate with sensitivity and risk, the University shall or shall require that its service provider implement inventory management practices that address the following components, at a minimum:

1. Associate a primary custodian to each IT asset.
2. Track IT asset transfers in a timely and accurate manner.
3. Identify the primary location(s) of each IT asset.
4. Require that digital media be sanitized prior to disposal. This process must occur in accordance with the *IT 5102 Data Storage and Media Protection Policy*.
5. Require creation and annual review of a list of University hardware and software assets.

10.3 Software License Management

10.3.1 Purpose

Software License Management requirements identify the steps necessary to protect against use of computer software in violation of applicable laws and contracts.

10.3.2 Requirements

The University shall or shall require that its service provider document and implement software license management practices that address the following components:

1. Assess annually whether all software is used in accordance with license agreements.

10.4 Configuration Management and Change Control

10.4.1 Purpose

Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during their life cycles. While the full extent of Configuration Management and Change Control is beyond the scope of this Standard, the University will establish and maintain a change control process.

10.4.2 Requirements

The University shall, or shall require that its service provider, document and implement configuration management and change control practices so that changes to the IT environment do not compromise existing security controls.

11 GLOSSARY

Access: The ability to use, modify or affect an information system or to gain physical entry to an area or location.

Access Controls: A set of security procedures that monitor access and either allow or prohibit users from accessing information systems, networks and data.

Alert: Notification that an event has occurred or may occur.

Application: An executable computer program.

Application System: An interconnected set of information resources under the same direct management control.

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Assurance: Measure of confidence.

Attack: An attempt to bypass security controls, disrupt services and/or gain unauthorized access to systems, networks and/or data.

Audit: An independent review and examination of records and activities to test for adequacy of controls, measure compliance with established policies and operational procedures, and recommend changes.

Authentication: The process of verifying the identity of a user to determine their access rights.

Authorization: The process of granting access after proper identification and authentication has occurred.

Availability: The extent to which data or information systems are available and accessible for authorized use.

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is unavailable.

Baseline Security Configuration: The minimum set of security controls that must be implemented on all University information systems to include vendor provided systems and hosted systems.

Broadcast Domain: A broadcast domain is a logical part of a network (a network segment) in which any network equipment can transmit data directly to another equipment or device without going through a routing device (assuming the devices share the same subnet and use the same gateway).

BIA Essential: Systems defined as supporting essential business functions in the Business Impact Analysis (BIA).

Business Function: A collection of related structural activities that produce something of value to the organization, its stakeholders, or its customers.

Business Impact Analysis (BIA): The process of determining the potential consequences of a disruption or degradation of business functions.

Change Control: A management process to provide control and traceability for all changes made to a system.

Chief Information Officer of the University (CIO): The CIO oversees the operations and overall security of the University's information systems, networks, and data as delegated by the University President.

Commonwealth of Virginia: The government of the Commonwealth of Virginia, and its agencies and departments.

Computer Security Incident Response Team (CSIRT): A group within the University constituted to monitor and respond to information security threats.

Confidentiality: The extent to which data must be protected against unauthorized disclosure to individuals or systems.

Configuration Management: A process for authorizing and tracking all changes to an information system during its life cycle.

Continuity of Operations Plan (COOP): A set of documented plans developed to provide for the continuance of essential business functions during an emergency.

Continuity of Operations Planning: The process of developing plans and procedures to continue the performance of essential business functions in the event of a business interruption or threat of interruption.

Control: Any protective action, device, procedure, technique, or other measure that reduces exposures. Types of controls include preventative, detective, corrective, etc.

Control Objectives for Information and related Technology (COBIT): A framework of best practices for IT management that provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control.

Credential: Information used to establish access rights. An example is a password.

Cryptography: The process of transforming plain text into cipher text (encryption), and cipher text into plain text (decryption).

Data: An arrangement of numbers, characters, and/or images that represent concepts symbolically.

Database: A collection of logically related data (and a description of this data), designed to meet the information needs of an organization.

Data Breach: The unauthorized access and acquisition of un-redacted computerized data that compromises the security or confidentiality of personal information.

Data Classification: The process of categorizing data based on sensitivity and risk.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: A University Manager, designated by the System Owner, who is responsible for the policy and practice decisions regarding data. Data owners approve or deny access to University data.

Data Security: Practices, technologies, and/or services used to apply security appropriately to data.

Data Storage Media: A device used to store data. Examples of data storage media include fixed disks, CDROMs, and USB flash drives. See media.

Decryption: Transform cipher text into human or machine-readable text.

Digital Certificate: An electronic document attached to or associated with a file that certifies the file is from the organization it claims to be from and has not been modified.

Disaster Recovery Plan (DRP): A set of documented plans that identify the steps to restore essential business functions on a schedule that supports the University's mission requirements.

Disaster Recovery Strategy: A strategy document that identifies the steps necessary for identifying and restoring essential business functions on a schedule that supports the University's mission.

Electronic Information: Any information stored in a format that enables it to be read, processed, manipulated, or transmitted by an information system.

Elevated Access Privileges: Privileges assigned when a user is granted access rights beyond that of a standard user.

Encryption: Transforming human or machine-readable text (often called plain text) into cipher text.

Essential Business Function: A business function is essential if disruption or degradation of the function prevents the University from performing its mission as described in the University's mission statement.

Evaluation: Procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

External IT System: An information system designed and intended for use by external parties and/or by the public.

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Full Tunneling: All network traffic goes through the tunnel to the organization. The University's VPN is an example of a full tunneling technology.

Function: A purpose, process, or role.

Fuzz Testing: This is a software testing technique that provides random data (”fuzz”) to the inputs of a program. If the program fails (for example, by crashing, or by failing built-in code assertions), the defects can be noted and perhaps further exploited (by security researchers or crackers) to gain elevated access to IT systems, networks or data.

Group: A named collection of information system users; created for convenience when stating authorization policy.

Guest Account: A default set of permissions and privileges given to nonregistered users of a system or service.

Hardening: The process of implementing software, hardware, or physical security controls to mitigate risk associated with University infrastructure and/or sensitive information systems, networks, and data.

Health Insurance Portability and Accountability Act (HIPAA): Enacted in 1996 to help protect health insurance coverage for workers and their families when employees change or lose their jobs. Provisions of HIPAA also address the security and privacy of health and patient data.

High Availability: A requirement that the information system is continuously available, has a low threshold for down time, or both.

Highly Sensitive Data: University data which, because of its potential risk in the event of disclosure, alteration or destruction, is approved for use only on a very limited basis and with special security precautions. This includes personally identifiable information that can lead to identity theft exposure.

Identification: The process of associating a user with a unique user ID or login ID.

Information: Data organized in a manner to enable their interpretation.

Information Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an information system, network or data.

Information Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system.

Information Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an IT system.

Information Security Logging: Chronological recording of system activities sufficient to enable the reconstruction, review, and examination of the sequence of events and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Information Security Officer (ISO): The individual designated by the CIO to be responsible for the development, implementation, oversight, and maintenance of the University's information security program.

Information Security (IS) Policy: A statement of the information security objectives of an organization, and what employees, contractors, vendors, business partners, and third parties of the University must do to achieve these objectives.

Information Security Program: A collection of security processes, standards, rules, and procedures that represents the implementation of an organization's security policy.

Information Security Requirements: The types and levels of protection necessary to adequately secure a system, network or data.

Information Security Safeguards: See Information Security Controls.

Information Security Standards: Detailed statements of how employees, contractors, vendors, business partners, and third parties of the University must comply with its information security policy.

Information Technology: Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology Contingency Planning: The component of Continuity of Operations Planning that prepares for continuity and/or recovery of the University's IT systems, networks, and data that support its essential business functions in the event of a business interruption or threat of interruption.

Information Technology Infrastructure Library (ITIL): A framework of best practice processes designed to facilitate the delivery of high-quality information technology services.

Information Technology Security: The protection afforded to IT systems, networks, and data in order to preserve their availability, integrity, and confidentiality.

Information Technology Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for IT systems, networks and data.

Information Technology Security Audit: The examination and assessment of the adequacy of IT system controls and compliance with established information security policy and procedures.

Information Technology Security Auditor: University Internal Auditors, the Auditor of Public Accounts, or a private firm that, in the judgment of the University, has the experience and expertise required to perform IT security audits.

Information Technology System: An interconnected set of IT resources under the same direct management control. See Application System and Support System.

Information Technology System Sensitivity: See Sensitivity.

Information Technology System Users: As used in this Standard, a term that includes University employees, contractors, vendors, third-party providers, and any other authorized users of IT systems, applications, telecommunication networks, data, and related resources.

Integrity: The extent to which data or information systems must be protected from intentional or accidental unauthorized modification or destruction.

Internal IT System: An IT system designed and intended for use only by University employees, contractors, and business partners. See Information Technology System and External IT System.

Internal IT System User: A University employee who uses an IT system in any capacity to perform job duties.

Internal Network: An internal network is a private computer network used to securely share any part of the University's information or operational systems with its employees.

Internet: An external worldwide public data network using Internet protocols to which the University can establish connections.

Intranet: A trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet protocols, which can be developed, operated and maintained for the conduct of University business, research, education, etc.

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts, either manually or via software systems.

Intrusion Detection Systems (IDS): Software that detects an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures to signal an alert. Others look for deviations of the normal routine as indications of an attack and are sometimes called anomaly detection systems.

ISO/IEC: A series of IT security standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), providing best practice recommendations on IT security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

IT Support Services: IT support services is a range of services providing assistance with technology products such as mobile phones, computers, or other electronic or mechanical goods. In general, technical support services attempt to help the user solve specific problems with a product rather than providing training, customization, or other support services.

Key: A sequence of data used in cryptography to encrypt or decrypt data. A password or passphrase is an example of a symmetric key. With symmetric keys, the exact same key encrypts and decrypts the data. With asymmetric keys, one key encrypts the data while a separate, different key decrypts it.

Least Privilege: The minimum level of data, functions, and capabilities necessary to perform a user's duties.

Logon ID: An identification code assigned to a particular user that identifies the user to the information system.

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, stealing, damaging, or destroying information systems and/or data. Malicious code includes viruses, Trojan horses, trap doors, worms, spy-ware, and counterfeit computer instructions (executables).

Malicious Software: See Malicious Code.

Management Control: A set of mechanisms designed to manage and achieve desired objectives.

Media: Plural of medium.

Media Sanitization: A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Medium: Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.

Minimum System Configuration: See Baseline Security Configuration.

Mobile Devices: Any computing device that can be easily transported and that has the capability to process and transmit data, including but not limited to laptops, smartphones, tablets, and handheld PCs.

Mobile Storage Devices: Any transportable storage device that can be used to store data including but not limited to portable hard drives and USB flash drives.

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

NIST: National Institute of Standards and Technology.

Non-Sensitive System: Systems not classified as sensitive.

Off-site Storage: The process of storing vital records in a facility that is physically remote from the primary site. To qualify as off-site, the facility should be geographically separate and distinct from the primary site and offer environmental and physical access protection.

Operational Controls: Information security measures implemented through processes and procedures.
Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Penetration Testing: A penetration test is a method of evaluating the security of a computer system or network.

Personal Digital Assistant (PDA): A digital device, which can include the functionality of a computer, a cellular telephone, a music player and a camera. Also called a smart phone.

Personal Identification Number (PIN): A short sequence of digits used as a password.

Personal Information (PI): All information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. "Personal information" shall not include routine information maintained for the purpose of internal office administration whose use could not be such as to affect adversely any data subject nor does the term include real estate assessment information. Code of Virginia 2.2-3801.

Personnel: All University employees, contractors, and subcontractors, both permanent and temporary.

Phishing: A form of criminal activity characterized by attempts to acquire sensitive information fraudulently, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication.

Privacy: The rights and desires of an individual to limit the disclosure of individual information to others.

Privacy Officer: The privacy officer, if required by statute (such as HIPAA) provides guidance on the requirements of state and federal Privacy laws; disclosure of and access to sensitive data; and security and protection requirements in conjunction with the information system when there is some overlap among sensitivity, disclosure, privacy, and security issues.

Protected Data: University data that is private or confidential, is not intended to be disclosed publicly, and/or is subject to state or federal regulation. Access to Protected data is granted on a need-to-know basis for a specific business use between University staff, IT systems, or other parties when authorized. Examples of Protected data include student data as defined as confidential by the Family Educational Rights and Privacy Act (FERPA), employee performance evaluations, confidential donor information, or other information defined by the University, Federal or State regulations as confidential.

Public Data: University data intended for general public use (e.g. university course listings, publicity and news articles, directory listings, etc.)

Public Web Site: A public web site is the most visible and readily accessible to the average Web user. A site on the Web that is accessible by anyone with a Web browser and access to the Internet.

Recovery: Activities beyond the initial crisis period of an emergency or disaster that are designed to return information systems and/or data to normal operating status.

Recovery Point Objective (RPO): The measurement of the point in time to which data must be restored in order to resume processing transactions. Directly related to the amount of data that can be lost between the point of recovery and the time of the last data backup.

Recovery Time Objective (RTO): The period of time in which systems, applications or functions must be recovered after an outage.

Residual Risk: The portion of risk that remains after security measures have been applied.

Restoration: Activities designed to return damaged facilities, equipment, systems and networks to an operational status.

Risk: The potential that an event may cause a material negative impact to an asset.

Risk Analysis: A systematic process to identify and quantify risks to information systems, networks and data and to determine the probability of the occurrence of those risks.

Risk Management: Identification and implementation of information security controls in order to reduce risks to an acceptable level.

Risk Assessment (RA): The process of identifying and evaluating risks so as to assess their potential impact.

Risk Mitigation: The continuous process of minimizing risk by applying security measures commensurate with sensitivity and risk.

Role Based Training: Specific annual training that addresses the roles and responsibilities of System Owners, Data Owners, Data Custodians and System Administrators. This training is in addition to annual IT Security Awareness training.

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This Standard contains the roles and responsibilities associated with implementing information security.

Secure: A state that provides adequate protection of information systems, networks, and data against compromise, commensurate with sensitivity and risk.

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for information systems, networks, and data.

Sensitive System: Systems where confidentiality, integrity or availability are rated as HIGH.

Sensitivity: A measure of the adverse affect on University interests, the conduct of University programs, and/or the privacy to which individuals are entitled that compromised information systems, networks, and data could cause.

Sensitivity Classification: The process of determining whether and to what degree information systems, networks and data are sensitive.

Shared Accounts: A logon ID or account utilized by more than one entity. An example of a shared account would be a University club account.

Source Code Auditing: A software (source) code audit is a comprehensive analysis of source code in a programming project with the intent of discovering bugs, security breaches or violations of programming conventions. It is an integral part of the defensive programming paradigm, which attempts to reduce errors before the software is released.

Split Tunneling: Routing organization-specific traffic through the VPN tunnel, but other traffic uses the remote user's default gateway.

Spyware: A category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

State: Commonwealth of Virginia.

Support System: An interconnected set of IT resources under the same direct management control that shares common functionality and provides services to other systems. See also Application System and Information Technology System.

System: See Information Technology System.

System Administrator: An analyst, engineer, or consultant who implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Classification: The process of categorizing systems based on confidentiality, integrity and availability.

System Owner: The University Manager who is responsible for the operation, documentation and maintenance of a University IT system. An IT System may have only one System Owner.

Technical Controls: Information security measures implemented through technical software or hardware.

Temporary Files: Files that are created as an application executes, but upon application termination, are no longer required for processing; nor are they part of the final representation of data.

The University: Radford University.

Third-Party Provider: A company or individual that supplies IT equipment, systems, networks or services to the University.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token: A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Trojan Horse: A malicious program that is disguised as or embedded within legitimate software.

Trusted System or Network: An IT system or network that is recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

Unique password: Passwords used must be separate and different from passwords used for any other university or commercial account.

Universal Serial Bus (USB): A standard for connecting devices to computers.

University: Radford University.

University President: The chief executive officer of the University.

USB Flash Drive: A small, lightweight, removable, and rewritable data storage device.

User ID: A unique symbol or character string that is used by an IT system to identify a specific user. See Logon ID.

Version Control: The management of changes to documents, programs, and other data stored as computer files.

Virus: See Malicious Code.

Vital Record: A document, regardless of media, which, if damaged or destroyed, would disrupt business operations.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Zero-Day (Zero-Hour) Attack or Threat: A computer threat that attempts to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available.

12 ACRONYMS

BIA: Business Impact Analysis

CIO: Chief Information Officer

COOP: Continuity of Operations Plan

DRP: Disaster Recovery Plan

DRS: Disaster Recovery Strategy

FERPA: Family Educational Rights and Privacy Act

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

ISO: Information Security Officer

ISO/IEC: International Organization for Standardization/ International Electrotechnical Commission

ITRM: Information Technology Resource Management

ITS: Information Technology Services

NIST: National Institute of Standards and Technology

PCI: Payment Card Industry

PDA: Personal Digital Assistant

PI: Personal Information

PIN: Personal Identification Number

RA: Risk Assessment

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SDLC: Systems Development Life Cycle Solutions Directorate

SSID: Service Set Identifier

SSP: System Security Plan