INFORMATION TECHNOLOGY SECURITY PROGRAM

Longwood University

Abstract

Standard for the Information Technology Security Program

STD-ITSP

In compliance with Incident Response Policy 6014, this plan will be reviewed annually.

Revision 25.11.4

Information Security Officer

infosec@longwood.edu

PREFACE

NOTICE

It is the reader's responsibility to ensure they have the latest version of this Standard. Revision questions should be directed to Longwood University's Information Security Officer (ISO). The most recent, approved version of this Standard will always be available upon request and on Longwood University's Information Security Office (InfoSec) Policies & Procedures website.

AUTHORITY

Memorandum of Understanding between Longwood University and the Commonwealth of Virginia code § 23.1-1003.

The Chief Information Officer (CIO), or designee, has approval authority over this Standard.

PURPOSE OF THIS STANDARD

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

GENERAL RESPONSIBILITY

The agency head has designated the ISO to develop information security policies, procedures, and standards to protect the confidentiality, integrity, and availability of Longwood University's information technology (IT) systems, networks, and data. Therefore, the ISO is the author and maintainer of this Standard.

SCOPE

This standard applies to all of Longwood University.

BASE STANDARDS

International Organization for Standardization and the International Electrotechnical Commission ISO/IEC 27000 series.

Center for Internet Security (CIS) Benchmarks Level 1

LONGWOOD UNIVERSITY
INFORMATION SECURITY

TABLE OF CONTENTS

INTRODUCTION

INTENT

The intent of this Standard is to establish a baseline for information security and risk management activities for all of Longwood 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.

Each component contains requirements that, taken together, comprise the Information Technology Security Program. 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.

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.

EXCEPTIONS TO SECURITY REQUIREMENTS

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

- The business need and justification
- The scope and extent of the deviation
- Mitigating safeguards
- The related risks
- The system owner's approval accepting residual risks

Each request shall be in writing to InfoSec using the IT Security Policy & Standard Exception Request Form.

EXEMPTIONS FROM THIS STANDARD

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

- 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.
- Surplus and retired systems.

ENFORCEMENT

Longwood University regards any violation of this policy as a serious offense. Violators of this policy are subject to disciplinary action, in addition to possible cancellation of IT resources and systems access privileges. Users of IT resources and systems at Longwood University are subject to all applicable local, state, and federal statutes. This policy does not preclude prosecution of criminal and civil cases under relevant local, state, federal and international laws and regulations.

ACCESS TO INFORMATION TECHNOLOGY RESOURCES AND SYSTEMS STANDARD

PURPOSE

This standard is to identify the requirements for granting, maintaining, and terminating users' access to Longwood University IT resources and systems.

STANDARD

Access to and use of Longwood University IT resources and systems will be limited to persons directly affiliated with the University. Exceptions to this limitation are permitted under certain conditions subsequently described.

LONGWOOD AFFILIATED:

- Learners: any persons enrolled, including full or part-time students and degree or non-degree seeking students, or those accepted into an established academic program.
- Professionals: any persons employed by, or retired from, Longwood University or Foundation, including:
    - Faculty holding either permanent or temporary appointments.
    - Adjunct Faculty
    - Instructors
    - Visiting Faculty
    - Staff holding either part-time or full-time positions.

Not Longwood Affiliated:

Access to and use of IT resources and systems by persons not directly affiliated with Longwood University must involve work to be performed, sponsorship and approval.

- Nature of the Work: Must satisfy at least one (1) of the following conditions:
  - the work relates directly to or is in support of Longwood University sponsored activities.
  - the work involves use of IT resources and systems available only from Longwood University and can be accommodated without disruption to established workloads.
- Sponsorship of Access: Requests for access by persons not directly affiliated with Longwood University must be sponsored by a professional of Longwood University who agrees to assume responsibility for use and adherence to the Acceptable Use of IT Resources and Systems Policy and maintains communication with Information and Instructional Technology Services (IITS) as necessary regarding the given access.
- Approval of Access: Requests must be submitted by the sponsor in writing to the CIO for approval. Requests must identify the person(s) needing access, describe the access needed, indicate the duration of the access (not to exceed 1 year), and provide contact information for the individual receiving access or the organization he or she represents.

GRANTING PRIVILEGES:

Access to IT resources and systems is granted only for the resources and systems that are necessary for an individual to perform his or her duties, is explicitly granted by the data owner or his or her designee to an individual and is assigned via a unique access account/ID. Authentication is required at the time of access through the use of a password, ID card, etc. (see Authentication Standard).

PRIVILEGED ACCESS:

Privileged access is defined as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the Power Users, Local Administrators, Domain Administrators and Enterprise Administrators groups would all be considered to have privileged access. In a traditional UNIX or Linux environment, users with root level access or the ability to sudo would be considered to have privileged access. In an application environment, users with system administrator roles and responsibilities would be considered to have privileged access.

- Use of Privileged Access: Privileged Access to IT resources and systems should only be used for official Longwood University business requiring the use of privileged access and should be consistent with a user's role or job responsibilities.
  - Longwood University business is not:
    - accessing restricted information that is outside the scope of specific job responsibilities.
    - exposing or otherwise disclosing restricted information to unauthorized

persons.
    - using access to satisfy personal curiosity about an individual, system or other type of entity.
    - without prior authorization, documented by management:
        - circumventing user access controls or any other formal Longwood University security controls.
        - circumventing bandwidth limits.
        - circumventing formal account activation/deactivation procedures.
        - circumventing formal account access change request procedures.
  - Accomplishing general day-to-day activities, such as e-mail and internet browsing/research, never require privileged access.
  - Install software from authorized and authoritative sites only. Abide by any license agreements for any software installed using the privileged access and be able to provide a copy of the license if requested.
- Authorization of Privileged Access: Privileged access will be granted on a system-by-system basis requiring approval from the System Owner, the ISO, and the user's supervisor, or designee (to include Third Party Contract Language). Privileged access is requested via the Privileged Access Request form.
  - Exemptions:
    - All users of the Faculty/Staff Workstation System have System Owner approval for privileged access; therefore, privileged access requires supervisor and ISO approval.
    - All users whose job requires specific Active Directory administrative group membership have System Owner approval for privileged access; therefore, privileged access only requires supervisor and ISO approval.
- Authentication Requirements: Supplementary and/or stronger authentication is required to utilize privileged access. As such, privileged access requires at least one of the following:
  - A unique-to-the-privileged-access password that meets the Password Management Standard as well as an abbreviated expiration, at a minimum of every 90 days.
  - Multi-factor Authentication via the Longwood University approved application.
- Termination of Privileged Access: When a user's role or job responsibilities change, privileged access should be promptly updated or removed.
- Enforcement: Violators of this standard are subject to disciplinary action, in addition to possible cancellation of privileged access.

PHYSICAL ACCESS:

The following rules are for the granting, controlling, monitoring and removal of physical access to Longwood University IT resources and systems facilities. These facilities include areas containing sensitive data and telecommunications equipment.

- All physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- All facilities must be physically protected in proportion to the criticality or importance of their function at Longwood University.

- Access to facilities must be granted only to authorized personnel whose job responsibilities require access to that facility.
- The CIO or his or her designee must authorize access to facilities.
- Access to facilities will be promptly terminated when the need for that access no longer exists. The CIO or his or her designee reserves the right to suspend and/or terminate any access privileges he or she determines to be a potential threat to the confidentiality, integrity or availability of any sensitive IT resources and systems.
- Individuals without authorized access privileges must be escorted by an Information and Instructional Technology Services staff member with authorized access to the facility for the duration of the visit.
- All access to the facilities must be logged.
- All incoming or outgoing equipment from a facility should be identified, inventoried and logged with documentation to include the Longwood University tag number, model number, date installed or removed and equipment description.
- At a minimum, access to facilities will be reviewed by the ISO on an annual basis.

REMOTE ACCESS:

Remote access is the ability to get access to Longwood University IT resources and systems without directly connecting to the Longwood University's wired network.

REMOTE ACCESS USAGE REQUIREMENTS:

- All computing devices used for remote access to the Longwood University IT resources and systems must adhere to:
  - the Malware Protection Standard,
  - Protecting Your PC,
  - Protecting Your Mac
  - and Protecting Your Smart Device.
- Non-Longwood University Owned Computing Device
  - Individuals remotely accessing Longwood University IT resources and systems from non-Longwood University owned computing devices may use:
    - Publicly available web-based applications
    - Web-based Virtual Private Network (VPN) with two-factor authentication via Remote Desktop Protocol (RDP)
    - WebEx service
- Longwood University Owned Computing Device
  - Individuals remotely accessing Longwood University IT resources and systems from Longwood University owned computing devices may use:
    - Publicly available web-based applications
    - VPN technology installed on the device with two-factor authentication
    - WebEx service
- Users remotely accessing Longwood University's IT resources and systems are responsible for selecting their own Internet Service Provider (ISP) and maintaining compliance with the contracts and policies of their ISP.
- Users must not attempt to bypass security controls implemented for remote access solutions, including inactivity time limits.
- Users should be aware that encryption technologies, which may be installed on devices used for remote access, are protected by U.S. government export restrictions. Further details may be found in the Encryption Standard.

- Eligible employees using non-Longwood University-owned computing devices for remote access must be aware of the requirements in the Information Technology Standard Use of Non-Commonwealth Computing Devices to Telework document from the Virginia Information Technologies Agency (VITA).

ACCOUNTABILITY:

The owner of an access account/ID is accountable for its use. It is the ID owner's responsibility to protect the integrity of accessible systems and preserve the confidentiality of accessible information as appropriate. Beyond the account/ID creation process any subsequent access to any discrete resources and/or data must be authorized by the appropriate data owner. Under no circumstances can the data owner, the data owner's authorized alternate or any other individual authorize access for him or herself.

TERMINATING ACCESS:

General Requirements:

Access will be promptly terminated when the need for that access no longer exists. The ISO or his or her designee reserves the right to suspend and/or terminate any access privileges he or she determines to be a potential threat to the confidentiality, integrity or availability of any sensitive IT resources and systems.

Specific Requirements:

- Professionals:
  - The Human Resources Office (HR) will be responsible for communication regarding the termination of access for faculty and staff as follows:
    - **Involuntary Termination**: HR must notify the Information Security Office via phone on or before the effective date of the involuntary termination to have access disabled and subsequently follow-up with ITS in writing or via e-mail on or before the effective date to have the access terminated.
    - **Voluntary Termination:** HR must notify ITS in writing or via e-mail on or before the effective date of the voluntary termination to have access terminated.
    - **Suspension:** Upon completing a review of any suspension action to be taken and deem the professional a security risk, HR must notify the Information Security Office in writing or via e-mail to have access suspended. Access will remain suspended from the effective date until written notification is received to reinstate it.
    - **Retirement:** HR must notify ITS in writing or via e-mail on or before the effective date of the retirement. Retirees have the option to retain e-mail access.
    - **Transfer Roles:** HR must notify the Information Security Office in writing or via e-mail a minimum of five business days before the effective date of the re-allocation, transfer or job function change. The Information Security Office will notify the user's previous manager that a re-allocation, transfer

or job function change has been identified and that the user must have his or her access re-validated by the appropriate data owner(s). All access not re-validated will be terminated no later than the effective date or following business day.
    - Termination of access will occur no later than the effective date or following business day.
    - Access will be terminated after a period of 12 months of account inactivity.

- Learners:
    - **Withdrawal, Graduation, Academic Suspension, etc.:** All access is removed when the appropriate notification is received via the enterprise resource planning (ERP) system. Termination of access will occur no later than the effective date or following business day.
    - **Work Study Access Expiration:** Access granted for learners as part of their employment by Longwood University will expire no later than the end of each academic year.
    - **Work Study Termination:** For any access granted to learners as part of their employment by the University, the sponsoring department will notify ITS in writing or via e-mail on or before the effective date of the termination. Termination of access will occur no later than the effective date or following business day.
    - **Immediate Suspension:** The Office of Vice President for Student Affairs will notify the Information Security Office in writing or via e-mail on or before the effective date of the suspension and again when access is to be reinstated. Access will remain suspended from the effective date until notification is received to reinstate it.

- Not Longwood affiliated:
    - **Expiration:** Access for not Longwood affiliated users will be terminated on the date indicated on the initial request form, unless renewed.
    - **Termination:** Sponsors are responsible for notifying the Information Security Office should a not Longwood affiliated user leave before the set expiration indicated on the initial request form.

ACCESS REVIEWS:

Commensurate with sensitivity and risk, all access will be reviewed periodically for accuracy by the data owner(s).

EXCEPTIONS AND EXEMPTIONS:

Exceptions to or exemptions from any provision of this policy must be approved in writing by the CIO or his or her designee.

AUTHENTICATION STANDARD

PURPOSE

The purpose of this standard is to ensure that the person supplying an identity is the person to whom the supplied identity has been assigned.

STANDARD

Authentication is the process of verifying the identity of users. Generally, it is accepted that the forms of authentication come in three types that may be used separately or together: something the user knows (e.g., a password), something the user carries (e.g., an ID card) or something about the user (e.g., a fingerprint).

The system owner or his or her designee for the system involved will, with input from data owner(s) and system administrator(s), make the decision about the level and type of authentication that will be deployed. The following types of authentications listed in order of strength are permitted for use on Longwood University systems:

- Network Address/Physical Location: May be used to restrict access to data or a particular service to persons using a specific networked device or any Longwood University networked device in general. "Proxy"-type services may be deployed where it is necessary to provide this access to University users who are not physically attached to a University network segment (e.g., library databases). An additional form of authentication will be necessary to ensure that the person accessing this proxy mechanism is indeed a member of the Longwood University community and as such authorized to access the network address-protected services.
- Personal Identification Number (PIN): PIN authentication will be available for use as a security measure for smart devices. The PIN must be a minimum of four digits. Users will be responsible for safeguarding the integrity of their PIN.
- Password: Passwords or passphrases may be used for applications where access to data or information systems requires individual or personal identification, and where this single password or passphrase is sufficient to authenticate this identity. Passphrases differ from passwords in that they are much longer (typically 20 to 40 characters) making them more secure against "dictionary attacks." The secure password or passphrase should be used for systems requiring a high level of individual accountability. See the Password Management Standard for more information on the use of passwords.
- Authentication Device: This level of protection makes use of password token technology in addition to a password, for systems requiring a higher level of individual accountability than a password alone can provide. The user must physically possess the device in addition to knowing the password associated with the account.
- Biometrics: Biometric authentication verifies a user's identity by requiring the capture of a biometric sample (e.g., fingerprint) and comparing that sample to a stored biometric sample that was enrolled by the user. This level of protection is appropriate for systems requiring a higher level of accountability than a password can provide and when a system for secure enrollment of users' biometric samples is present.

All information used for authentication, either stored or in transit, must be protected. The data must be encrypted according to the Encryption Standard. Only the minimum amount of access necessary should be granted to allow the authentication process to function.

DATA CLASSIFICATION STANDARD

PURPOSE

The purpose of this standard is to identify how the sensitivity of Longwood University's data will be classified. Sensitivity is the degree of adverse effect a compromise of confidentiality, integrity or availability would have on Commonwealth of Virginia interests, the conduct of Longwood University programs or the privacy to which individuals are entitled.

STANDARD

Longwood University data owners, as defined in the Information Security Roles and Responsibilities Standard, will be responsible for identifying all types of data handled by the University and classifying the sensitivity of the data. In determining the sensitivity of the data, the requirements of federal, state, and local laws must be considered.

CLASSIFICATION OF DATA

- Data will be classified based on the following:
  - Public data is the least sensitive information and is acceptable for public consumption.
  - Internal data is moderately sensitive information. All Longwood University data is considered Internal unless classified otherwise.
  - Restricted data is highly sensitive information for which an unauthorized disclosure may result in identity theft or Longwood University liability for costs or damages under laws, government regulations or contract.
- Data owners are required to follow the instructions and format approved by InfoSec for conducting and completing their data classification. This includes an initial classification and the re-classification of data at least annually.
- Data Classifications will be publicly available.
- Users will be responsible for the data they handle and adhering to the Data Handling Standards prescribed to consistently protect the data throughout its life cycle and in any form.

PROCEDURES

DATA HANDLING STANDARDS

Data owners may impose additional security controls/protections needed for a type of data, in addition to the controls required by the classification level.

- Classification Label:
  - Public:
    - Confidentiality: Low
    - All Longwood University data acceptable for public consumption.
    - Disposal:
      - Electronic data:
        - Delete
      - Non-electronic data:

        - Recycle
- Internal:
    - Confidentiality: Medium
    - All data used for conducting Longwood University business that is not meant for distribution beyond the University. All University data is considered "Internal" until classified otherwise.
    - Storage:
        - Electronic data: Not publicly accessible
        - Non-electronic data: Secure location with appropriate physical controls
    - Disposal:
        - Electronic data:
            - Delete
            - Redact
        - Non-electronic data:
            - Redact
            - Shred with cross-cut shredder*
- Restricted:
    - Confidentiality: High
    - All Longwood University data for which an unauthorized disclosure may result in identity theft or University liability for costs or damages, under laws, government regulations or contract.
    - Storage:
        - Electronic data:
            - Data owner's approval
            - Not publicly accessible
            - Encryption required
        - Non-electronic data:
            - Data owner's approval
            - Secure location with appropriate physical controls
            - Labeled at data owner's discretion
    - Transmission:
        - Campus Mail: Secured and labeled at data owner's discretion
        - External Mail: Secured and labeled at data owner's discretion
        - Electronic Transmission: Encryption required (internal and external** e-mail, file transfers, VoIP, etc)
    - Disposal:
        - Electronic data:
            - Redact
            - Make unreadable/unrecoverable per Electronic Data Disposal Standard
        - Non-electronic data:
            - Redact
            - Shred with cross-cut shredder*

*Per Virginia Administrative Code: Note: Although you may not have a cross-cut shredder, as long as the shredded records are pulped or incinerated, it meets the requirements of the regulations that Social Security Numbers in the records be made, "...unreadable or undecipherable by any means."

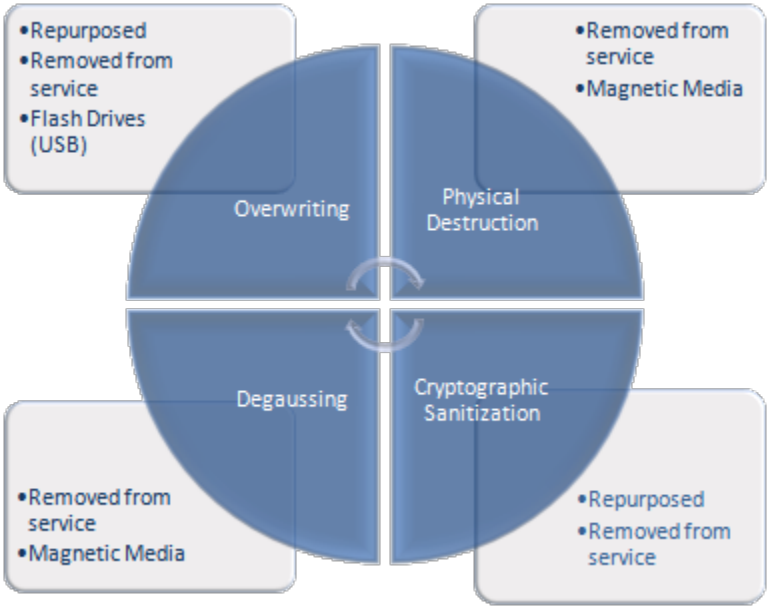
**External e-mail containing Social Security Numbers (SSN) and/or Credit Card Numbers (CCN) are prohibited.

ELECTRONIC DATA DISPOSAL STANDARD

The intent of this standard is to minimize the risks of exposing data to unauthorized individuals and inadvertently transferring software to those not licensed to use it. Removing from service and/or repurposing any Electronic Data Storage Device (EDSD) or computer software creates risks for Longwood University. These risks can include unauthorized disclosure of data and the violation of software license agreements, copyrights or other intellectual property that might be stored. Any EDSD, especially those containing restricted data, must have all data sanitized prior to disposal as specified by these standards and the terms of any licensed software.

Electronic Data Storage Device (EDSD): Any device requiring electrical power to be capable of storing and/or processing data, such as those containing volatile memory and/or magnetic or optical storage. This includes but is not limited to hard drives of personal computers, servers, mainframes, Personal Digital Assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, cell phones, smart phones, printers, multifunction devices, digital cameras, flash memory cards or SD cards, and Universal Serial Bus (USB) data storage devices.

Cycle Matrix of Data Disposal:



Standards Matrix of Data Disposal:

		Overwriting	Cryptographic Sanitization	Degaussing	Physical Destruction	Battery Removal
Functional						
In service	Repurposed	•	•			
Removed from service	Surplus value	•	•			
	No surplus value*	•	•	•	•	
Non-Functional				•	•	
Volatile Memory						•

*includes EDSDs from which data cannot be removed.

The sanitization of data must be performed on an EDSD in a manner that gives assurance that the data cannot be read and/or recovered.

1) All EDSDs shall be sanitized at the earliest time after being taken out of use but not later than 60 days.
   a) Multi-user EDSDs, such as lab and loaner pool computers, will be sanitized between users as time permits, but not less than annually.
2) All documentation and communication must be completed as outlined in bullet point 5 for any EDSD.
3) The method used for data disposal depends upon the functional state of the EDSD.
   a) A Functional EDSD that will be repurposed or removed from service and has surplus value shall be overwritten or cryptographically sanitized prior to disposal. If the EDSD is to be removed from services and has no surplus value, it shall be overwritten, cryptographically sanitized, physically destroyed, or degaussed.
   b) If the EDSD is non-functional, it shall be physically destroyed or degaussed.
   c) Data stored in volatile memory, in both functional and non-functional EDSDs, shall be disposed of as outlined in bullet point 4.e.
4) The following bullet points outline the acceptable methods of data disposal from any EDSD.
   a) Overwriting: Overwriting of data means replacing previously stored data with a predetermined pattern of meaningless information. The overwriting process, including the software products and applications used for the overwriting process, shall be capable of:
      i) Overwriting the entire EDSD, independent of any limitation that the EDSD may have, making it impossible to read and/or recover any intelligible data.
      ii) Overwriting a minimum of one pass of pseudo random data or zeros on all sectors, blocks, tracks, and any unused disk space on the entire EDSD.
      iii) Verifying that all data has been sanitized. This verification can be either a separate process or included as part of the software used for overwriting.
         (1) Verification on flash memory, to include USB data storage devices and solid-state drives, shall be suspect.
         (2) If data is not completely overwritten, and sanitization fails verification, then overwriting is not an acceptable method of data disposal, and another approved method must be applied.
   b) Degaussing: Degaussing is a process whereby the magnetic media is sanitized. EDSDs seldom can be used after degaussing. Please note that extreme care should be used when using degaussers since this equipment can cause damage to nearby telephones, monitors, and other EDSDs. Also, the use of a degausser does not guarantee that all data

on the EDSD will be sanitized. The following steps shall be followed when EDSDs are degaussed:

i) Follow the product manufacturer's directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing.
ii) Shielding materials (cabinets, mounting brackets), which may interfere with the degaussing equipment magnetic field, shall be removed from the EDSD before degaussing.
iii) Hard disk platters shall be degaussed during the degaussing process in accordance with the manufacturer's specifications.

c) Physical Destruction: Physical destruction shall be accomplished to an extent that precludes any possible restoration of the data. The following steps shall be followed when EDSDs are destroyed:
   i) Cut the electrical connection to the EDSD.
   ii) Shielding materials (cabinets, mounting brackets), which may cause injury during EDSD destruction, shall be removed from the EDSD before destruction begins.
   iii) The EDSD should then be subjected to physical force or extreme temperatures that will disfigure, bend, mangle or otherwise mutilate the EDSD so it is unreadable. Acceptable means of destruction include:
      (1) pulverization (pounding with a sledgehammer)
      (2) incineration and melting
      (3) shredding and disintegration
      (4) Multiple holes drilled into the hard disk platters.
   iv) Destruction by end users is not recommended. CD-ROM discs do not require extensive destruction. Discs that are outdated or no longer needed may be rendered unreadable by cutting in half or deep scratching the data side (the shiny side without the label) with a nail, screwdriver, or similar tool. Two deep radial scratches extending from the small inner hole to the outer edge are sufficient to prevent unauthorized access to the data. These discs may be placed in the general waste stream for disposal.

d) Cryptographic Sanitization: Sanitization by cryptography works by first encrypting all data as it is written to the EDSD. The only way to read or recover data protected in this manner is to use a valid decryption key. Instant and thorough sanitization occurs when the decryption key is destroyed. See the Longwood University Encryption Standard.

e) Data Disposal from Volatile Memory Media: Any EDSD that holds data or configurations in volatile memory shall have all data sanitized by either the removal of the battery or electricity supporting the volatile memory or by such other method recommended by the manufacturer for an EDSD where the battery is not removable. This often includes computer equipment that has memory such as personal computers, PDAs, routers, firewalls, and switches.

5) Documentation and Communication: Any disposal action, including certifying that the data has been effectively disposed of, shall be completed in accordance with the following:

a) The following information regarding the data disposal process shall be documented prior to an EDSD being removed from service and/or repurposed and communicated to the new user/consumer:
   i) All individually identifiable Number(s), such as Asset Tag Number(s), Serial Number(s), etc. that are uniquely associated with the EDSD from which data is being sanitized.
   ii) The type of EDSD from which data is being sanitized.
   iii) The date of the data disposal.
   iv) The method(s) used for data disposal.
   v) The name of the person responsible for the data disposal.

vi) The name and signature of the person's supervisor.

b) The completed documentation shall be maintained in a secure location and available for audit.

c) The communication to the new user/consumer shall accompany the sanitized EDSD. Communication must include one of the following:

i) Certification Tagging:

(1) Certification Tags may be printed on a label that is size-appropriate to the EDSD. Preferably the tags will be printed in red letters for ease of recognition.

(2) Certification Tags must be affixed to the EDSD such that:

(a) For individual EDSDs such as hard drives, or PDAs, and networked appliances, a certification tag shall be affixed to each EDSD.

(b) For multiples of EDSDs such as CDs, tapes, etc. a certification tag shall be completed for each physically aggregated lot by affixing the certification tag to the storage container or shrink-wrapped pallet. Lots must be aggregated when there is more than one person per function per lot (i.e. more than one data disposer, or more than one quality assurance tester, etc.).

(3) Acknowledgement via "Terms of Use" (Data Disposal Certification in a document signed by the new user/consumer.)

Other related procedures may be maintained internally by Information Technology Services (ITS).

ENCRYPTION STANDARD

PURPOSE

The primary purpose of this standard is to protect restricted data, as defined by the Data Classification Standard, by limiting the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively while setting standards for all use of encryption, and to identify federal exportation regulations regarding encryption technologies.

STANDARD

Proprietary Encryption: An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual or the government.

Encryption Key: A piece of information used to encode or decode data with a cryptographic algorithm.

- All use of encryption technology must be managed in a manner that permits properly designated Longwood University officials prompt access to all data, including for purposes of investigation and business continuity.
  - Encryption keys and their backups must be retained for the lifetime of the encrypted data.
  - Encryption key management procedures must be in place to ensure integrity and recovery of encryption keys.
- No encryption technology other than that approved and distributed by ITS may be used to protect restricted data.

- ITS will provide:
  - Minimum Encryption Standards
  - Encryption Key Management Standards
- Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application.
- The use of proprietary encryption algorithms is not allowed, unless reviewed by qualified experts outside of the vendor in question and approved by the Information Security Office.
- Acknowledgement of Federal Exportation Regulations: Be aware that the export of encryption technologies is restricted by the U.S. government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

MINIMUM ENCRYPTION STANDARDS

Symmetric Cryptosystem: A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem: A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

One-way Hash Function: An algorithm that does not require a key and produces an irreversibly encrypted cipher-text. Other names for this algorithm are message digest, fingerprint, digital signature, and compression function.

Restricted data which is encrypted and stored on Longwood University managed resources and/or systems should have:

- Symmetric cryptosystem key lengths that must be at least 128 bits
- Asymmetric cryptosystem keys that must be of a length that yields equivalent strength.

Restricted data which is encrypted by Longwood University managed resources and/or systems for transmission should use:

- Web server certificates and web servers which support SSLv3/TLSv1 in strong encryption mode (128 bit or higher symmetric/bulk encryption, 1024 bit or higher public key encryption)
  - For public facing resources: Certificates must be issued by a trusted certificate authority as approved by the CIO.
  - For non-public facing resources: Self-signed certificates may only be used for the purpose of managing such resources.
- SSL to wrap any cleartext protocol/service not encrypted via another method
- SSH 2
- Kerberos
- PCAnywhere
- PGP
- Terminal Services
- EAP, IPSec
- WPA2

ENCRYPTION KEY MANAGEMENT STANDARDS

Encryption Key: A piece of information used to encode or decode data with a cryptographic algorithm.

Encryption Keys and their backups must be:

- handled in a manner that permits properly designated Longwood University officials (Internal Audit, Information Security, and/or Campus Police) prompt access to all data, including for purposes of investigation and business continuity,
- physically secured when stored or transmitted offline,
- stored or transmitted separately from the data protected by the encryption key,
- and retained for the lifetime of the data being protected.

Related policies, standards and guidelines may be maintained internally by ITS.

FIREWALL STANDARD

PURPOSE

This standard provides the configuration, maintenance, control, and monitoring of enterprise-wide firewall technology used to safeguard Longwood University's IT resources and systems.

STANDARD

Firewall Technology: Any combination of network hardware, network software and host-based software used within an organization to prevent unauthorized access to system software or data.

Outbound Connection: An outbound connection allows University network users to utilize Internet services.

Inbound Connection: An inbound connection allows Internet and external IP network users to reach the University's networks.

- Longwood University's enterprise firewall technology provides a degree of separation between layers and prevents unauthorized access from a less trusted layer to a more trusted layer. From outermost (least trusted) to innermost (most trusted), the layers are:
    - Internet and other external IP networks
    - Perimeter networks (varies according to level of trust)
    - Internal network (the most trusted network)
- Firewall technology will inspect network traffic to determine if the requested connection should be permitted or denied.
    - Outbound connections (more trusted to a less trusted layer) are generally permitted by default.
    - Inbound connections (less trusted to more trusted layer) are denied by default.
- The system administrator of a system located on a more trusted network may request in writing a firewall "rule" to allow access (inbound connections) from a system on a less trusted network to a more trusted network. The ISO must approve all rule requests.
    - Temporary or testing access requests must include a reasonable expiration date not to exceed 30 days at a time.

    - Requests for access to student owned systems will be valid for only one academic year at a time and will be automatically removed each May after graduation.
    - Requests for access to faculty and staff systems from the Internet are not allowed.
- Firewall technology will be configured to use system logging.
- Daily operation and maintenance of firewall technology will be the responsibility of the Communication and Telephony Services (CTS) department.
- CTS will review firewall configurations annually or in the event of a situation warranting review of the configuration. Examples of such situations are (but not limited to):
    - The implementation of major enterprise computing environment modifications.
    - Any occurrence of a major information security incident.
    - New applications are being considered or applications are being phased out or upgraded.
- The ISO or his or her designee reserves the right to review, modify or revoke any rule requests or configuration changes at his or her discretion.

INFORMATION SECURITY ROLES AND RESPONSIBILITIES STANDARD

PURPOSE

This Standard defines the key IT security roles and responsibilities included in the Information Technology 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, if 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.

DESIGNATION OF ROLES

- All security roles will be designated in such a way that allows for separation of duties and prevents conflict of interests.
    - The ISO is not a system owner or a data owner except in the case of compliance systems for information security.
    - The system owner and the data owner are not system administrators for IT systems or data they own.
- Designations of security roles and assigned responsibilities must be documented:
    - for employees, in their Position Description or Employee Work Profile.
    - for system vendors in their contract.
- Responsibilities of individuals in security roles will be reviewed annually.
- Any individual designated as system owner and/or data owner must be an active, management level employee.

CHIEF INFORMATION OFFICER (CIO)

The CIO is accountable for directing the information and data integrity of the enterprise to include:

- Reporting data breaches to the Office of the Attorney General or to the Commissioner of Health without unreasonable delay.
- Working with senior management when contacting external agencies or authorities regarding an incident, as defined in Incident Response.
- Designating an alternate, as relevant to Incident Response.

INFORMATION SECURITY OFFICER (ISO)

The ISO is responsible for developing and managing the IT security program to include:

- Developing and managing an IT security program in accordance with the Information Technology Security Program Policy.
- Developing and maintaining a security awareness and training program in accordance with the Security Awareness and Training Standard.
- Ensuring that all Longwood University data and IT systems are classified for sensitivity.
- Implementing and maintaining an appropriate balance of protective, detective, and corrective controls for IT systems commensurate with data sensitivity, risk, and systems' criticality.
- Designating a single system owner for each IT system.
- Designating Incident Response Coordinator(s), certified in incident response, as approved by the ISO.
- Designating an alternate, as relevant to Incident Response.
- Documenting the responsibilities for each role.
- Reviewing System Security Plans:
    - Approving System Security Plans that provide adequate protections against IT security risks; or
    - Disapproving System Security Plans that do not provide adequate protections against security risks and require the system owner implement additional security controls on the IT system to mitigate those security risks.
- Assist in the determination of investigative goals during an incident, as defined in Incident Response.

SYSTEM OWNER

A system owner is responsible for the operation and maintenance of the IT system(s) they own, to include:

- Managing system risk and developing any additional procedures required to protect the system in a manner commensurate with risk.
- Determining the investigative goals during an incident, as outlined in the Incident Response Plan.
- Ensuring compliance with applicable policies and standards.
- Ensuring compliance with requirements specified by data owners for the handling of data processed by the system.
- Designating system administrators:
    - Each system will have at least two system administrators.
    - Security tasks may be divided between application security and infrastructure

security which may be assigned to different individuals.
    - Any individual designated as a system administrator for infrastructure must be either a member of ITS staff or a vendor.
- Designating the data owners for any data created or shared within their division.

DATA OWNER

A data owner is responsible for the policy and practice decisions regarding data he or she owns, to include:

- Evaluating and classifying the sensitivity of the data.
- Defining the protection requirements for the data based on the Data Classification Standard and/or business needs.
- Communicating data protection requirements to the system owner.
- Defining requirements for access to the data.
- Determining the investigative goals during an incident, as outlined in the Incident Response Plan
- Designating a data custodian for the data.

INCIDENT RESPONSE TEAM (IRT)

An IRT is responsible for the investigation of incidents, as outlined in the Incident Response Plan, to include:

- Collecting and analyzing evidence to determine the threat and subsequent containment of the incident.
- Documenting individual actions during an incident.

INCIDENT RESPONSE COORDINATOR (IRC)

An IRC is responsible for assembling and managing an IRT during the investigation of an incident, as outlined in the Incident Response Plan, to include:

- Serving as a liaison between the ISO and the IRT.
- Ensuring that system and data owner investigative goals are met, and special handling instructions and priorities are adhered to.
- Ensuring evidence is properly collected, documented, and secured.

SYSTEM ADMINISTRATOR

A system administrator is responsible for implementing, managing and/or operating a system, for which he or she has been assigned, at the direction of the system owner, data owner and/or data custodian to include:

- Managing and documenting vulnerability scans.

- Implementing security controls and other requirements of the security program.
- Reporting security events per the Incident Response Policy.

DATA CUSTODIAN

A data custodian is responsible for the physical or logical data for which he or she has been assigned to include:

- Protecting the data from unauthorized access, alteration, removal, or usage.
- Establishing, monitoring and operating systems in a manner consistent with security policies and standards.
- Providing, administering, and documenting general controls, such as backup and recovery systems.

PRIVACY OFFICER

A privacy officer is responsible for directing Longwood University's adherence to state or federal privacy law (e.g., FERPA, HIPAA) to include:

- Providing guidance on the requirements of the laws or regulations, including limits on disclosure of and access to sensitive data.
- Advising the University on the adoption of security protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.

USER

All members of the Longwood University community are responsible for the protection of the confidentiality, integrity, and availability of University data to include:

- Adhering to the Data Handling Standards to consistently protect the data throughout its life cycle and in any form.
- Knowing, understanding, and abiding by the following:
  - Virginia DHRM Policy No. 1.75: Use of the Internet and Electronic Communication Systems
  - Policy 6002: Acceptable Use of Information Technology Resources and Systems
  - Policy 6023: Password Management
  - Policy 6014: Incident Response
  - FERPA

INFORMATION TECHNOLOGY SECURITY AUDITS STANDARD

PURPOSE

The purpose of this standard is to establish a Longwood University IT security audit baseline to assess whether IT security controls implemented to mitigate risks are adequate and effective.

STANDARD

The University's Internal Audit department shall develop risk-based audit programs to assess, evaluate, and make recommendations to management regarding the adequacy of internal controls inherent in the University's information systems, and the effectiveness of the associated risk management. The IT audit function assesses the extent to which automated information processing systems, technology, architecture and processes produce reliable and accurate information, are in accordance with the University's policies and procedures, and applicable laws and regulations. To gain adequate coverage over design and operating effectiveness, Internal Audit plans IT assessments over a three-year cycle.

INFORMATION TECHNOLOGY SYSTEMS DEVELOPMENT LIFECYCLE STANDARD

PURPOSE

The purpose of this standard is to establish a Longwood University IT systems development life cycle to offer consistency and structure to the IT systems development process and to ensure that security is considered throughout an IT system's development.

STANDARD

Systems Development Life Cycle (SDLC): The SDLC is a process for developing IT systems that offers consistency and structure in the progression of an IT system from concept to implementation to disposition.

ESTABLISHMENT OF THE SDLC

The SDLC is described in detail and will be followed for all Longwood University IT systems.

INITIATING THE SDLC

All new IT systems developed will enter the SDLC at the Planning Phase when a request for a new IT system or significant modification to an existing IT system is made through the Project Management Office's established IT project request procedures. New IT systems or significant modifications include those developed at the University or acquired from a third party.

CONSIDERATION OF SECURITY IN THE SDLC

Security will be integrated into each phase of the SDLC. An IT System Security Plan will be updated and maintained throughout the life cycle of an IT system.

PHASES OF THE SDLC

The SDLC process is a phased process, and phases will be completed in the order specified:

PLANNING

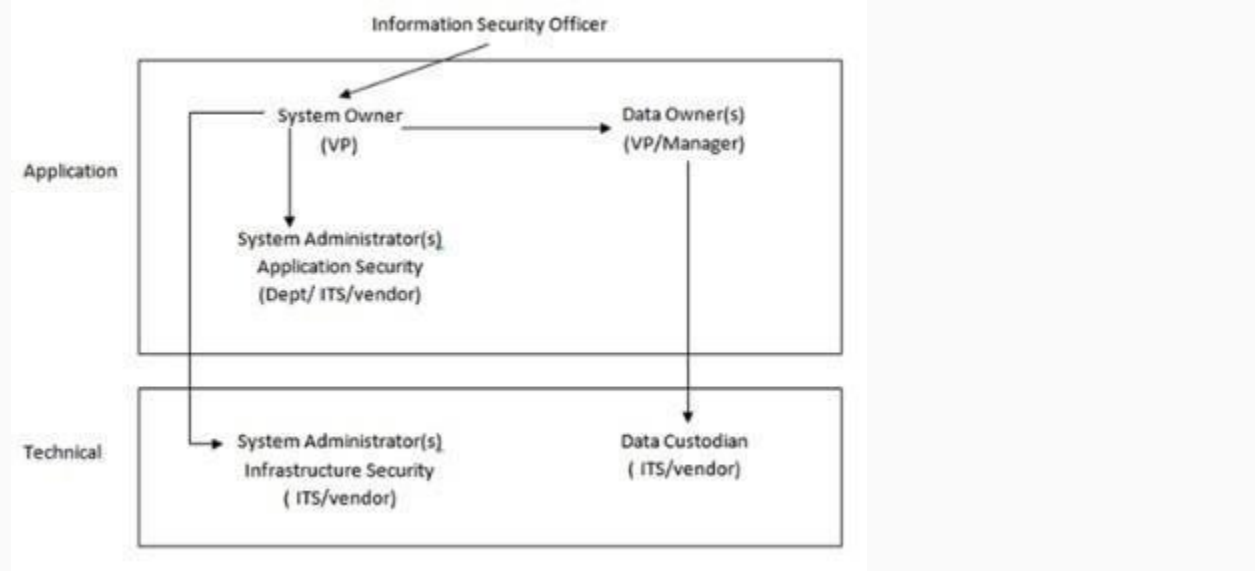
Requests for IT systems are developed into a Project Plan through the steps delineated by the Project Management Office.

INITIATION

Identify IT System Security Responsibilities based on the Information Security Roles and Responsibilities Standard.

Security roles and responsibilities are assigned:

- The ISO designates a system owner.
- The system owner designates the system administrator(s) and the data owner(s).
- The data owner(s) designate the data custodian.



Identify Risks and Controls:

- The system and data owner(s) or their designees perform an initial risk analysis based on initial requirements and objectives to establish security guidelines for system developers.
- The data owner(s) classifies the types of data the IT system will process and classify the

data's sensitivity.
    - For any data classified as sensitive the need for collection and maintenance of that data is re-evaluated.
    - Sensitivity of the IT system is determined by the sensitivity of the data.
- For any system identified as sensitive, the system owner develops an initial draft of the IT System Security Plan that documents the controls that the system will enforce to provide protection against identified risks.
- Classes of security controls:
    - Management Controls
    - Operational Controls
    - Technical Controls
- The IT System Security Plan is reviewed by the Information Security Office.

DEFINITION AND CONSTRUCTION

Design IT System Characteristics:

- The physical characteristics of the IT system are designed during this phase. The operating environment is established, inputs and outputs are defined and processes are allocated to resources.
- Design specifications for the security requirements of the IT System Security Plan are developed and documented.
- Everything requiring user input or approval is documented and reviewed by the user. The physical characteristics of the IT system are specified and a detailed design is prepared.

Develop IT System:

The detailed specifications produced during the design phase are translated into hardware, communications, and executable software. Software components are unit tested, integrated, and retested in a systematic manner. Hardware is assembled and tested.

- The incorporation of the security controls into the IT system design is verified and documented in the IT System Security Plan.
- At the discretion of the ISO, the ISO or his or her designee tests for proper and effective functioning of the security controls that may be tested prior to deployment. (Certain non-technical controls may not be effectively tested until the IT system is deployed.)

INTEGRATION AND TEST

Integrate IT System Components:

- All IT system components (hardware, communications, software, security controls) are incorporated and systematically tested.

Test Functionality and Security:

- The user ensures that the IT system's functional requirements are satisfied by the

developed system.
- The IT system undergoes any necessary certification and accreditation activities.
- InfoSec conducts an IT system security evaluation to ensure that the security requirements, as defined in the IT System Security Plan, are satisfied by the developed or modified IT system.
- The IT system security controls are accepted by the system owner.

IMPLEMENTATION

Make IT System Operational:

- The IT system or IT system modifications are installed and made operational in a production environment.
- This phase continues until the IT system is operating in a production environment in accordance with the defined design specifications and security requirements.

Document Risks and Controls:

- The system owner and data owner(s) or their designees will conduct a risk assessment of the system.
- The system owner or his or her designees will document the final IT System Security Plan to document the security controls implemented.
- The completed IT System Security Plan is approved by the ISO.

OPERATIONS AND MAINTENANCE

Continue Operation of IT System:

- With the IT system operation ongoing, the IT system is monitored for continued performance in accordance with design specifications and security requirements. Operations continue if the IT system can be effectively adapted to respond to an organization's needs.
- The IT system is periodically assessed through In-Process Reviews to determine how the IT system can be made more efficient and effective.
- The security controls are periodically assessed through security evaluations.

Modify IT System:

- Needed modifications are incorporated into the IT system.
- When major modifications or changes are identified, the IT system may reenter the Planning Phase.
- The IT System Security Plan will be updated by the system owner to document any changes to security controls implemented for the system and approved by the ISO. The IT System Security Plan will be reviewed and approved no less than once a year for restricted systems and once every three years for non-restricted systems.

DISPOSITION

When a decision is made to cease use of an IT system the following requirements must be met in the disposition:

Make Data Retention Decisions:

- Data handled by the IT system will be retained in accordance with Longwood University and/or Commonwealth of Virginia record retention requirements.

Dispose of the IT System Components:

- Electronic media will be sanitized, and hardware and software disposed of in accordance with Longwood University and/or Commonwealth of Virginia requirements.

DEFINITIONS

- Data: Data is an arrangement of numbers, characters and/or images representing information, knowledge, facts, concepts, or instructions.
- Data Owner: A Longwood University employee designated as responsible for the policy and practice decisions regarding data.
- Management Controls: A set of mechanisms designed to manage organizations to achieve desired objectives.
- Operational Controls: IT security measures implemented through policies and procedures.
- Risk Analysis: A systematic process to identify and quantify risks to IT systems and data and to determine the probability of the occurrence of those risks.
- Risk Assessment (RA): The process of identifying and evaluating risks so as to assess their potential impact.
- Security Evaluation: Procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific IT system weaknesses.
- Sensitivity Classification: The process of determining whether and to what degree IT systems and data are sensitive.
- Security Controls: The protection mechanisms prescribed to meet the security requirements specified for an IT system.
- Sensitive Data: Sensitive data is any data in print or electronic form of which a compromise of confidentiality, integrity or availability would have a significant and noticeable impact on the University's achievement of its mission.
- System: IT systems are interconnected sets of IT resources, including application systems which meet a defined set of business needs and support systems that provide services to other systems.
- System Owner: A Longwood University employee designated as responsible for the operation and maintenance of a University IT system.
- Technical Controls: IT security measures implemented through technical software or hardware.

MALWARE PROTECTION STANDARD

PURPOSE

The purpose of this standard is to protect Longwood University IT resources and systems from the introduction of malware.

Malware: Malware, short for malicious software, is any software designed to damage, disrupt, harm, or compromise any computer, server or network. Viruses, worms, trojans, rootkits, bots, and spyware are all various forms of malware.

STANDARD

All Longwood University users and IT resources and systems must operate in a way that protects against malware.

PREVENTION OF MALWARE:

- Users should not intentionally develop or experiment with malware on Longwood University's network.
- Users should not intentionally spread malware on Longwood University's network by:
    - Failing to run and maintain malware protection software.
    - Improperly using operating systems and or software updates.
    - Arbitrarily opening e-mails, specifically:
        - opening e-mail attachments within said e-mails.
        - clicking on links within said e-mails.
        - responding to said e-mails with requested personal information (phishing emails).
    - Arbitrarily opening files contained on portable media.
    - Failing to validate links, "hover over", when navigating the internet.
- Due to possible software vulnerabilities, users should not install software on Longwood University managed computing devices unless prior authorization is granted by the ISO or his or her designee.

DEPLOYMENT OF MALWARE PROTECTION:

- All Longwood University managed computing devices, whether connected to the University network or standalone:
    - must utilize Information and Instructional Technology Services (IITS) approved malware protection software and configuration.
    - must maintain malware protection software and configuration such that the software is not removed, disabled, bypassed, or altered in a manner that will reduce the effectiveness of the protection.
- All non-Longwood University computing devices, while connected to the University network, must utilize adequate malware protection software.
- All E-mail sent and received by Longwood University's mail system will be examined for malicious code.

EXCEPTIONS AND EXEMPTIONS:

- Exceptions to or exemptions from any provision of this policy must be approved in writing by the ISO or his or her designee.

PASSWORD MANAGEMENT STANDARD

PURPOSE

Effective password management is the most central single element in assuring the overall security of Longwood University IT resources and systems and the protection of University data. The purpose of this policy is to ensure that all users are aware of their responsibilities in effective password management and to ensure that appropriate password standards are applied to all Longwood University IT systems.

This standard applies to all IT systems whether connected to the network or standalone, hosted internally or externally or administered by ITS or another department.

Password Management: Password management is the selection, distribution, use, modification and testing of computer system passwords.

STANDARD

All who participate in the use and administration of Longwood University's IT resources and systems share responsibility for effective password management. Specific responsibilities are assigned as follows:

- Password Standards: Passwords will be required on all University sensitive IT systems and other IT systems where passwords are necessary for accountability, as well as on University mobile devices (e.g., smart phones). IITS will provide Minimum Password Standards that must be applied to all University IT systems that utilize passwords for authentication; however, more rigorous password requirements will be applied to IT systems commensurate with the systems' sensitivity and risk. The actual password requirements applied to the IT system will be documented in the IT system security plan.
- Password Testing: IITS reserves the right to monitor the overall security of The University's IT environment by testing the strength of passwords on all University IT systems, both those it administers and others.
- Personal Ownership of Password Management: Ultimately, individuals using The University's IT resources and systems are responsible for assuring effective password management. To fulfill this responsibility, they shall be aware of and follow the Minimum Password Standards. Most notably, this includes creating strong passwords and safeguarding their passwords' integrity. Passwords represent an individual's identity to the IT system and should never be disclosed to or used by others.

- Responsibility to Report Compromise: All users are required to immediately contact the Help Desk and change their password if at any time they suspect their password has been compromised.

EXEMPTIONS AND EXCEPTIONS

The ISO must approve exceptions to or exemptions from any provision of this policy or the Minimum Password Standards in writing.

MINIMUM PASSWORD STANDARDS

- LancerNet passwords must:
  - be at least 15 characters.
  - meet at least 3 out of the 4 requirements for quality:
    - at least (1) lower case letter
    - at least (1) upper case letter
    - at least (1) number
    - at least (1) special character (?, *, %, etc.)
  - be changed, at a minimum, every 120 days.
  - be unique:
    - Users should create a different username and password for external services such as personal e-mail, banks, music services, stores, personally owned computers or other systems.
    - Users should not repeat previous passwords and accordingly an encrypted record of previously used passwords will be maintained.
- LancerNet passwords must not:
  - be known or used by others.
    - Users must never provide their password to anyone.
    - Users must log off from applications when done using them.
    - Users must secure workstations when they are away from them. Devices will be subject to lockouts for inactivity.
    - Users must never use the "Remember Password" feature of any applications.
  - be all or part of your LancerNetID
  - be all or part of the IT system's name,
  - be blank,
  - be based on a single dictionary word,
  - contain more than (2) repetitive characters (e.g., Mmmmmmm1, Ab7777777, etc.),
  - be based on a simple keyboard combination (e.g., Qwerty).
- Non-Single Sign-On (SSO) Longwood University IT System password management
  - All University IT systems that do not authenticate via SSO should follow LancerNet Password standards.
- Users must report suspected password compromises.
  - Users must contact the Help Desk if they believe someone has obtained their password.

- Users must change their password if they suspect it has been compromised.

SECURITY AWARENESS AND TRAINING STANDARD

PURPOSE

The purpose of this standard is to identify the conditions necessary to provide IT system users with appropriate awareness of system security requirements and of their responsibilities to protect IT resources and systems.

IT system users in this context means faculty, retired faculty, staff, Longwood University Foundation employees, retired staff, student workers and any other individuals approved for access by the CIO.

STANDARD

Requirements:

- InfoSec will provide an online Security Awareness Training course and/or live workshops.
- Attendance and monitoring:
  - Documentation is required for all IT security training,
  - Training must be completed within 30 days of: (1) access being granted to IT resources and systems or (2) the assignment of role-specific security responsibilities; and all assigned training is required at least annually thereafter.
  - Annual training must be completed by October 31st of the calendar year.
  - InfoSec is responsible for monitoring receipt of IT security training.
  - InfoSec is responsible for enforcement of the requirements.

ENFORCEMENT

EMPLOYEES

- Area vice presidents will be notified of users who have yet to complete the training no later than October 15.
- Users' access will be suspended on November 1st (or within 3 business days).
- The user will be responsible for notifying ITS to have access re-enabled for a one-week grace period to complete all training.
- Users' access will be suspended if the training is not completed by the end of the grace period.

RETIREES

- Users' access will be suspended on November 1st (or within 3 business days).
- The user will be responsible for notifying ITS to have access re-enabled for a one-week grace period to complete all training.
- Users' access will be suspended if the training is not completed by the end of the grace period.

EXCEPTION (NOT-LONGWOOD AFFILIATED) USERS

- Sponsors will be notified of users who have yet to complete the training no later than October 15.
- Users' access will be suspended on November 1st (or within 3 business days).
- The user will be responsible for notifying ITS to have access re-enabled for a one-week grace period to complete all training.
- Users' access will be suspended if the training is not completed by the end of the grace period.

SECURITY LOGGING AND MONITORING STANDARD

PURPOSE

This standard provides the core of the security log management framework used to detect security events that pose a threat to IT resources and data. The intent is to log events that may appear innocent in isolation, but when viewed as part of a pattern may be determined to be malicious. Monitoring and logging are also crucial to security investigations and to ensure that IT security controls are in place and not being bypassed.

STANDARD

Core Business – Applications, systems, and network devices vital to the University's mission and business functions that are dependent upon the services provided by the core infrastructure.

Core Infrastructure – Applications, systems and network devices that support other systems or applications by providing essential services. (Examples include Active Directory, DNS, DHCP, routers, switches, etc.)

Log – Is a record of the events occurring within an organization's systems and networks. Logs contain information related to specific events that have occurred within a system or network.

Public-facing – Applications, systems, and network devices accessible from the internet and available to the public; also called customer facing.

Windows Event Viewer – Tool to view Windows OS logged events as well as 3rd party software written to send logs to the Event Viewer.

REQUIREMENTS:

- System administrators will develop logging procedures for systems they administer.
- Logging:
  - All Endpoints will be monitored, and logs collected through the detection and response platform.
  - Key Windows and syslog events to monitor:
    - Any changes to System files or folders ACLs.
    - Registry Changes.
    - Local and Domain Account changes.
    - Windows and SSH login success or failures.
    - Anti-virus logs.
    - Windows Event Log aggregation.

        - Access to network infrastructure.
        - Changes to ACLs on switches, router, or firewalls.
        - Web server access.
        - HTTP "404" errors.
        - FTP server access and file transfers.
        - Server security log events.
    - Key Windows Event logging categories to enable:
        - Logon events – Success/Failure.
        - Account logons – Success/Failure.
        - Account management – Success/Failure.
        - Directory Service access –Failure.
        - System events – Success/Failure.
- Log Event Management Solution:
    - Logging facilities and log information will be protected against tampering and unauthorized access to include:
        - Alterations or deletions to logs that are recorded.
        - Storage capacity of the log file media being exceeded, resulting in the failure to record events or over-writing of past-recorded events.
    - Log Event Management must meet the following requirements:
        - Automate collection of log files.
        - Ability to query log data for specific log event activity for analysis.
        - Secure log aggregation and storage for Windows Event logs and syslog data from devices and OS's.
        - Supports SQL and Oracle database log data.
        - Agent monitoring (Windows, MAC OS, and Linux).
        - Real-time monitoring.
        - Ability to create custom "alerts" for log monitoring.
    - NetFlow Data
    - Automatically collect NetFlow data from core router switches for analysis
- Logs will be maintained according to the Library of Virginia Data Retention schedule.

WIRELESS COMMUNICATION STANDARD

PURPOSE

This standard covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Longwood University's networks. This includes any form of wireless communication device capable of transmitting data over a network. Wireless devices and/or networks without any connectivity to the University's networks do not fall under the purview of this policy

STANDARD

Access Point: An access point is a piece of hardware that serves as a common connection point for devices on a wireless network and connects to the wired network allowing wireless access to the campus network.

IMPLEMENTATION OF WIRELESS ACCESS

- All wireless services in use at Longwood University will be supported, maintained and protected by Information and Instructional Technology Services (IITS) for use by its faculty, staff, students and any other authorized individuals.
- Wireless networking is provided as a supplement to wired networking, but due to issues including bandwidth and reliability wireless networking is not a substitute for wired connections.

PROTECTION OF WIRELESS SERVICES

All users of Longwood University wireless services should be aware that IITS will implement the following standards for protecting wireless services:

- Will maintain encryption between the data communication device and the access point.
- May register and track a hardware address (ex. MAC address) of those devices accessing the network.
- Will prohibit physical access to wireless access points by anyone other than authorized IITS staff.
- Will support the use of The University's virtual private network (VPN) technology. Further details may be found in the Remote Access Standard.

EXPECTATIONS OF USE

Due to its dependence on a scarce and shared resource, radio communication is subject to additional rules concerning interference and shared use.

- Interference or disruption of authorized wireless communications or unauthorized interception of any wireless communications is prohibited.

CHANGE LOG

- Update “ACCESS TO INFORMATION TECHNOLOGY RESOURCES AND SYSTEMS STANDARD” 11/4/2025 JDT
- Document creation: 10/9/2024 JDT