UNC
INFORMATION
TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Information Security Policy

General Policy Statement

All University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to campus who have access to University-owned or managed information through computing systems or devices ("Users") must maintain the security of that information and those systems and devices.

Basic "minimum" requirements apply to all University-owned or managed information and systems and devices. These can be found in the attached Information Security Standards.

More extensive requirements apply to Sensitive Information and Mission-Critical Resources. These are discussed below and in the Procedures and Standards documents which are found in the attached Information Security Procedures and Information Security Standards.

These Policies, Procedures, and Standards may be amended from time to time. Users will be notified of amendments through campus-wide email messages and announcements on the web site for Information Technology Services.

Scope

This policy and the related Procedures and Standards set forth security practices necessary to protect the UNC network and information. This policy does not supersede any applicable state or federal laws regarding access to or disclosure of information.

Audience

This policy applies to all Users accessing the UNC network or UNC information through computing devices owned by or managed through UNC-Chapel Hill or through permission granted by UNC-Chapel Hill. All Users must read this Policy Statement and the related Procedures and Standards in their entirety. If you have any questions about whether this Policy Statement applies to you or how it applies to you, please contact the University's Information Security Office at 919-445-9393.

Compliance

Failure to adhere to this Policy and the Procedures and Standards may put University information assets at risk and may have disciplinary consequences for

employees up to and including termination of employment. Students who fail to adhere to this Policy and the Procedures and Standards will be referred to the Honor System. Contractors and vendors who fail to adhere to this Policy and the Procedures and Standards may face termination of their business relationships with the University.

Policy on Sensitive Information

Sensitive Information, as defined below, in all its forms – written, spoken, electronically recorded, or printed – must be protected from accidental or intentional unauthorized modification, destruction, or disclosure. This policy statement addresses specifically the risks to privacy inherent in digital technologies.

The University requires all Users to protect the University's Sensitive Information by adhering to the attached Procedures and Standards as they may be amended from time to time.

Users with access to Sensitive Information must also adhere to the following policies:

- General User Password Policy
- Policy on the Transmission of Protected Health Information and Personal Identifying Information
- Protocol for Responding to Security Breaches of Certain Identifying Information
- Incident Management Policy
- Vulnerability Management Policy
- UNC-Chapel Hill Campus Standards for Electronic Media Disposal
- Security Liaison Policy

Users who are third-party contractors and vendors must be made aware of this policy and their responsibilities for safeguarding the University's Sensitive Information.

Sensitive Information: Sensitive Information includes all data, in its original and duplicate form, which contains:

- "Personal Identifying Information," as defined by the North Carolina Identity Theft Protection Act of 2005. This includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital

signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources.

- "Protected Health Information" as defined by the Health Insurance Portability and Acountability Act (HIPAA).
- Student "education records," as defined by the Family Educational Rights and Privacy Act (FERPA).
- "Customer record information," as defined by the Gramm Leach Bliley Act (GLBA).
- "Card holder data," as defined by the Payment Card Industry (PCI) Data Security Standard.
- Confidential "personnel information," as defined by the State Personnel Act.
- Information that is deemed to be confidential in accordance with the North Carolina Public Records Act.

Sensitive Information also includes any other information that is protected by University policy or federal or state law from unauthorized access. Sensitive Information must be restricted to those with a legitimate business need for access. Examples of Sensitive Information may include, but are not limited to, Social Security numbers, system access passwords, some types of research data (such as research data that is personally identifiable or proprietary), public safety information, information concerning select agents, information security records, and information file encryption keys.

Information Classification

All Users must be aware of the classification of the various types of University information to which they have access in order to determine the proper controls for safeguarding the information. Regardless of classification, the integrity and accuracy of all information must be protected. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, printed report) must have the same classification regardless of format. Only two levels are to be used when classifying information:

(1) Sensitive Information: **"**Sensitive Information" is defined above. It is important to note that the unauthorized disclosure of Sensitive Information to individuals without a business need for access may violate laws or University policies and may have significant ramifications for the University, its employees, its students, or its business associates.

Decisions about the provision of access to Sensitive Information must always be made by the Steward (as defined below) of that Sensitive

Information.

(2) Public Information: Public Information includes all information made or received by the University that does not constitute Sensitive Information. Sensitive Information that is disclosed without proper authorization does not, by virtue of its disclosure, become Public Information.

Many Users will find that some of the information to which they have access has been classified as Sensitive Information (e.g., employment records, student records) and some of it as Public Information (e.g., most purchase contracts, most accounting records).

Roles and Responsibilities

In addition to knowing the classification of each piece of University information to which they have access as either "Sensitive Information" or "Public Information," Users must be aware of whether, with respect to that information, they serve as a Steward, a Custodian, a Consumer/User, a User Manager, or an Information Security Liaison, as described within this Policy.

Steward of Information or Data: The Steward is the University employee responsible for the approval of the creation of a collection of information or data or the primary user of that information or data. For example, the Registrar is the Steward for much of the University's student information. The Vice Chancellor for Human Resources is the Steward for much of the University's employee information.

Custodian of Information or Data: The Custodian is responsible for the processing and storage of information or data on behalf of the Steward of that information or data.

Consumer/User: A Consumer/User is any person authorized to read, enter, copy, query, download, or update information.

User Managers: A User Manager is any University administrator, faculty member, or staff member who supervises Consumer/Users or who handles University business unit administrative responsibilities. User Managers are responsible for overseeing their Consumer/Users' access to Sensitive Information, including:

- Reviewing and approving all requests for access authorizations.
- Initiating security change requests to keep security records current so they

accurately reflect each Consumer/User's role and required access.

- Ensuring that the approved procedures are followed for employee suspensions, terminations, and transfers, and that appropriate measures are taken to revoke access privileges.
- Revoking access privileges from students, vendors, consultants, and others when access is no longer necessary or appropriate.
- Providing the opportunity for training needed to properly use computer systems.
- Reporting promptly to the Executive Director and Information Security Officer and to the Office of University Counsel any potential or actual unauthorized access of University Sensitive Information (security breach) in accordance with the University's Protocol for Responding to Security Breaches of Certain Identifying Information.
- Initiating appropriate actions when Information Security Incidents are identified in accordance with the Incident Management Policy.
- Ensuring that any Information Security requirements are followed for any acquisitions, transfers, and surplus of equipment that processes or stores electronic information, such as computers, servers, smartphones/PDAs, and certain copiers.

Information Security Liaison: Each University business unit that is responsible for maintaining its own information technology services must have a designated Information Security Liaison as well as a designated backup Information Security Liaison. The duties and responsibilities of the Security Liaison are described in detail in the Security Liaison Policy.

Key responsibilities for the individuals serving in each of the above roles are discussed in the Information Security Procedures and Standards, which are attached. In addition, the University's Executive Director and Information Security Officer will work with Stewards, Custodians, User Managers, Consumer/Users, and Information Security Liaisons to develop and implement prudent security policies, procedures, and controls, in consultation with the Office of University Counsel. The responsibilities of the Executive Director and Information Security Officer and the staff of the Information Security Office include:

- Developing an Information Security Strategy approved by the Chief Information Officer.
- Developing and maintaining a University Information Security Program to provide enterprise services for:

  Network Security
  Endpoint Protection
  Vulnerability Management

Information Security Consulting
Information Security Policy and Standards
Enterprise Information Security Awareness Initiatives
Enterprise Security Design and Architecture
Defining Information Security Requirements

- Serving as the University HIPAA Security Officer.

Policy on Mission-Critical Resources

Mission-Critical Resources, as defined below, must be protected from accidental or intentional unauthorized modification, destruction, or disclosure.

The University expects members of its faculty, staff, and student body to understand and mitigate the risks to privacy inherent in digital technologies. The University also requires members of its faculty, staff, and student body to protect the University's Mission-Critical Resources by adhering to the Procedures andStandards attached. Users who are third-party contractors and vendors must also be made aware of this policy and their responsibilities for safeguarding the University's Mission-Critical Resources.

Mission-Critical Resource: A Mission-Critical Resource includes any resource that is critical to the mission of the University and any device that is running a mission-critical service for the University or a device that is considered mission critical based on the dependency of users or other processes. Mission-critical services must be available. Typical mission-critical services have a maximum downtime of three consecutive hours or less. Mission-Critical resources for Information Security purposes include information assets, software, hardware, and facilities. The payroll system, for example, is a Mission-Critical Resource.

Mission-critical computer systems and the infrastructure required to support them must be installed in access-controlled areas. In addition, the area in and around a computer facility housing Mission-Critical Resources must afford protection against fire, water damage, and other environmental hazards, such as power outages and extreme temperature situations.

Each University business unit housing Mission Critical Resources is required to establish procedures to provide emergency access to those Resources in the event that the assigned Custodians or Stewards are unavailable, or when operating in an emergency.

Additional responsibilities for individuals working with Mission-Critical Resources

are discussed in the Information Security Procedures and Standards, which are attached.

Related Documents

For additional information on the University's information security policies, procedures, standards, and practices, please see:

- Information Security Procedures
- Information Security Standards
- Data Governance Policy
- Vulnerability Management Policy
- Incident Management Policy
- Policy on the Transmission of Protected Health Information or Personal Identifying Information
- General User Password Policy
- UNC-Chapel Hill Campus Standards for Electronic Media Disposal
- Security Liaison Policy
- Protocol for Responding to Security Breaches of Certain Identifying Information
- Definition of Sensitive Information

Contact Information

Subjects	Contact	Phone	Fax
Policy Questions Report a Violation Request Information Security Consulting	The University's Information Security Office	919-445-9393	919-445-9488

History

Effective Date:

Revised Date: 6/30/10; 6/28/11

Next Review Date: This policy will be reviewed at least annually.

Information Security Procedures

Maintaining the Security of Information throughout its Lifecycle

All Users (faculty, students, staff, temporary employees, contractors, outside vendors, and visitors to campus) must determine:

(1) whether they have access to information or data that constitutes the University's "Sensitive Information," as defined above, and
(2) whether they have responsibility for "Mission-Critical Resources" as defined above.

Anyone who has access to Sensitive Information or responsibility for Mission-Critical Resources **must** read, understand, and adhere to the following Procedures.

Definitions

Peer-to-Peer (P2P) Applications: P2P applications or filesharing technology, for Information Security purposes, is any application used for distributed communication that employs technology or communicates over the network in a way that is not under the complete control of the University at all times. P2P applications are tools used to facilitate communication or the transfer of information.

Vulnerability Scans: Scans using established scanners to detect vulnerabilities specific to database management systems, operating system and common application flaws and weaknesses (including missing system patches and misconfigurations), and web-based applications.

Procedures

All University-owned or managed systems and information/data are assets of the University. The security of these systems and information/data must be maintained according to these Procedures and the Information Security Standards. The required controls may be physical and/or software based.

1. The Creation, Transmission, Use, Maintenance, and Disposal of Sensitive Information

A. Creation of Sensitive Information

When creating Sensitive Information, the Steward of that information is

required to adhere to the Sensitive Information protection standards outlined in the Information Security Standards document. Any system storing or processing Sensitive Information must be documented and tracked by the Information Security Liaison in accordance with the Security Liaison Policy**.** Information must be documented and shared, upon request, with the Information Security Office.

Sensitive Information must at all times be protected against possible unauthorized access. Responsibility for Sensitive Information may be delegated by the Dean, Division Head, or their designee. Any delegation of responsibility must be clearly identified in writing as such. Stewards and Custodian(s) of Sensitive Information must be documented and tracked at all times by the Information Security Liaison.

B. Transmission of Sensitive Information

- The transmission of Sensitive Information, by email or otherwise, must be done with great attention to protecting the privacy of the information. Protected Health Information and Personal Identifying Information must be transmitted in accordance with the requirements outlined in the Policy on the Transmission of Protected Health Information and Personal Identifying Information and any applicable federal and state law.
- Sensitive Information must **never** be handled through Instant Messaging (IM) or Peer-to-Peer (P2P) filesharing software or devices. In addition, P2P software is not allowed to be installed on systems that store or process Sensitive Information.
- When storing Sensitive Information on a shared-network location, network share must adhere to all standards outlined in the Information Security Standards. For network shares, the Steward specifies the security controls and access rights. The Custodian implements the security controls and access rights in accordance with the Steward's specifications and consistent with the Information Security Standards. Consumer/Users will access Sensitive Information in accordance with University Policies and any applicable regulatory framework.
- Any defective electronic device or media transferred to a third party for replacement or repair must be preceded by a properly executed and signed Business Associate Agreement (if protected health information is involved) or a similarly binding document to safeguard the University's Sensitive Information.

C. The Use and Maintenance of Sensitive Information

- The storage of Sensitive Information on external devices must follow the standards outlined in the Information Security Standards document.
- Sensitive Information must not be stored on mobile devices or disposable media devices except in accordance with the Information Security Standards. Additionally, PHI and PII may only be stored on laptops, smartphones/PDAs, and other mobile devices if encrypted. This will limit the danger of unauthorized access in the event that devices storing Sensitive Information, including PHI or PII, are lost or stolen. (See Section 4 of this document for further information.)
- Any computing devices, such as workstations or servers, must be physically secured, password-protected, and encrypted, if required by the Information Security Standards.
- Adequate control mechanisms, such as privacy screens, must be in use when displaying Sensitive Information in areas accessible to unauthorized persons and when displaying Sensitive Information on frequently-viewed devices.
- Any publication of Sensitive Information must be in accordance with University Policies and any applicable federal and state law. In addition, any such publication must have the advance written approval of the respective Dean or Division Head with consultation, as necessary, with the Office of University Counsel. Sensitive Information must not be uploaded to or posted on any web site, including web sites maintained by the University, unless it is protected in a way that permits the Sensitive Information to be accessed and seen only by those individuals authorized to access and see it.
- Restoring Sensitive Information from backup devices must be in accordance with Section 7 of this Policy on Backup & Recovery.
- Verbal communication of Sensitive Information must be in accordance with federal and state law. When verbally communicating Sensitive Information to other authorized personnel, individuals must be aware of their surroundings to prevent unauthorized disclosure of Sensitive Information.
- Any other use of Sensitive Information, whether in duplicate or original form, must be in accordance with University Policy, including the Information Security Standards and the Policy on the Transmission of Protected Health Information and Personal Identifying Information.

D. The Permanent Deletion and Destruction of Sensitive Information

The destruction of Sensitive Information must be in accordance with departmental record retention schedules and consistent with the standards defined in the UNC-Chapel Hill Campus Standards for Electronic Media Disposal. Any department intending to surplus devices that process or store electronic information, such as computers, servers, smartphones/PDAs, and certain copiers, must, in accordance with the UNC-Chapel Hill Campus Standards for Electronic Media Disposal, first destroy the electronic information by wiping, then keep the devices physically secure until the devices are in the possession of University Surplus personnel. In addition:

- Hard copy (paper and microfilm/fiche) documents containing Sensitive Information must be disposed of by shredding.
- All forms of media used to store electronic data (e.g., floppy disks, hard drives, CD-ROMs, optical disks) must be permanently deleted or destroyed in accordance with the UNC-Chapel Hill Campus Standards for Electronic Media Disposal. Any physical destruction must be performed by University Surplus.

2. Software Used for University Business Purposes

Any software used to conduct University business must comply with all Information Security policies and standards. Software used for business purposes should, in most cases, be owned by the University and reside on University-owned systems or devices. In the cases where one or the other of these is not the case, but University business is conducted, all policies and standards must still be followed.

3. Access Controls

Physical and electronic access to Sensitive Information and computing resources must be controlled. Access controls must be defined by the Steward and implemented by the Custodian of the Sensitive Information. For further consultation or questions regarding the appropriate access controls, contact the Executive Director and Information Security Officer.

Mechanisms to control access to Mission-Critical Devices and Sensitive Information include (but are not limited to) the following methods:

A. Authorization

Access controls should be appropriate to the sensitivity of the data as outlined in the Information Security Standards. For consultation on the appropriateness of access controls, contact the Executive Director and

Information Security Officer.

B. Identification/Authentication

Unique user identification (user id) and authentication is required for all systems that store, process or access Sensitive Information. Consumer/Users will be held accountable for all actions performed on the system with their user identification. For more detailed information, see the General User Password Policy.

At least one of the following authentication methods must be implemented as outlined in the Information Security Standards:

- Passwords conforming to the General User Password Policy,
- Biometric identification technology as approved by the Executive Director and Information Security Officer, and/or
- Multi-factor authentication issued in conjunction with private information (e.g., a smart card combined with a password).

Consistent with the General User Password Policy and, to the greatest extent technically possible, an automatic timeout re-authentication must be required after a certain period of inactivity. The maximum period of inactivity is 30 minutes unless the User(s) has a business reason for a longer period, as approved by the Executive Director and Information Security Officer.

Where physical security controls cannot ensure that access to a system that stores or processes Sensitive Information is restricted to a single authorized individual, the Consumer/User must lock the system when leaving it unattended for an extended period of time to prevent unauthorized access and ensure accountability.

C. Remote Access

Sensitive Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the University network. For detailed standards, consult the Information Security Standards and the Policy on the Transmission of Protected Health Information and Personal Identifying Information.

D. Physical Access

Access to areas in which Sensitive Information is stored must be controlled by a Custodian of that Sensitive Information. Only authorized personnel may access secure areas and only when there is a legitimate business need. The following physical controls must be in place:

- Mission-Critical computer systems and the infrastructure required to support them must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards, such as power outages and extreme temperature situations.
- Likewise, servers on which Sensitive Information is stored must be kept in a secure area to protect against unauthorized access. Logs should be maintained to record entries and exits from the secure area.
- Computing Devices that contain or have access to Sensitive Information, including any mobile devices, must be secured against use, including viewing, by unauthorized individuals. In particular, workstations and mobile devices must be positioned to minimize unauthorized viewing of Sensitive Information. Physical safeguards, such as locating workstations in controlled-access areas or installing covers or enclosures, should be employed to preclude passerby access to Sensitive Information.
- Sensitive Information must not be stored on mobile devices or disposable media devices without compliance with the Information Security Standards. In addition, Sensitive Information must never be stored on mobile devices or disposable media unless those devices have been issued and are property of, or managed by, UNC-Chapel Hill and storing UNC-Chapel Hill's Sensitive Information on a mobile device is required to fulfill an important business need.
- On rare occasions and only with written approval of the Dean or Department Head and pursuant to a written contract with an outside third party, mobile devices belonging to UNC business partners or vendors may be used to store or access UNC-Chapel Hill's Sensitive Information, as long as the non-UNC third party contractually accepts the responsibility for maintaining the security of the University's Sensitive Information in accordance with all the Information Security Standards.

E. Emergency Access to Mission-Critical Devices and Data

Each University business unit is required to establish procedures to provide emergency access to Mission-Critical Devices and applications in the event that the assigned Custodians or Stewards are unavailable, or when operating in an emergency.

F. Audit Controls

Detailed audit logs that document electronic access to Sensitive Information should be kept for the duration specified in any applicable records retention policy, but generally not less than 90 days. Logs should be periodically reviewed or alerts set on logged information to detect any unauthorized access. The University requires that audit processes be implemented to examine logged information in order to identify questionable data-access activities, investigate breaches, respond to potential weaknesses, and assess the security program.

4. Data Transfer/Printing

A. Electronic Data Transfers

Technical security mechanisms must be employed to guard against unauthorized access to Sensitive Information that is transmitted over a communications network. When transmitting Sensitive Information to third parties, such as outside vendors, a signed contractual or formal business agreement with the third party, approved by the Office of University Counsel, must be in place that ensures the protection of Sensitive Information and clarifies the liability for any data compromise or security breach. Downloading and uploading Sensitive Information between systems must be strictly controlled. Protected Health Information or Personal Identifying Information may only be transferred in accordance with the University's Policy on the Transmission of Protected Health Information and Personal Identifying Information.

B. Printing and Faxing

Sensitive Information must not be copied, printed, or stored in a manner that would leave it vulnerable to unauthorized access.

5. Storage of Sensitive Information on Other Media

The physical security of Sensitive Information stored on any external media (e.g., diskette, CD-Rom, portable storage, memory stick) must be maintained at all times. Sensitive Information stored on external media must be protected from unauthorized access consistent with the standards described herein and in the Information Security Standards. External media and mobile computing devices containing Sensitive Information

must never be left unattended in unsecured areas.

As described in the Information Security Standards, Sensitive Information must never be stored on mobile computing devices (e.g., laptops, personal digital assistants (PDA), smart phones, tablet PCs) unless approved in writing by the head of the Division (e.g. Dean or Vice Chancellor) and unless these devices are University owned or managed and maintained in compliance with the Information Security Standards. These provisions apply to any systems or devices regardless of whether the devices are owned or managed by the University or personally-owned.

6. Incident Management

Each University business unit that manages its own or subcontracts its information technology is required to establish and maintain an up-to-date incident management plan as described in the Incident Management Policy. The Information Security Office reserves the right to remove a user's network access in order to mitigate the risk to the UNC-Chapel Hill network during an Information Security Incident. Network access will be removed for users if their continued access of UNC-Chapel Hill network resources has the potential to impact the security and availability of the UNC-Chapel Hill campus network and information technology resources.

In addition, the Information Security Office has the right to take over IT management for any University business unit that consistently fails to address serious vulnerabilities or information security incidents within a reasonable time in order to bring the business unit's IT operations into compliance with these Procedures and the Information Security Standards.

7. Vulnerability Management

Each University business unit maintaining computing resources storing Sensitive Information or maintaining Mission-Critical Resources must perform monthly vulnerability scans in accordance with the Vulnerability Management Policy. Any detected vulnerabilities must be remediated based on the specific timeframe described in the Vulnerability Management Policy.

8. Backup & Recovery

Custodians of information/data must ensure that the systems and information for which they are responsible are recoverable within a reasonable time period. Each University business unit operating Mission-Critical Resources is required to develop and maintain a plan for

responding to a system emergency and to Information Security Incidents. These plans must include performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster, as described in the Information Security Standards.

- Backup media must be encrypted and protected as described in the Information Security Standards. A disaster recovery plan must be developed and documented in coordination with the University's Business Continuity Office. This includes the development and documentation of an emergency mode operation plan.
- Backup data/media must be periodically stored in a secure off-site location and remain protected as described in the Information Security Standards. Off-site storage locations should be compliant with the commercial standards for environmental controls.
- Any secure backup that requires the transmission of Protected Health Information or Personal Identifying Information must be performed in compliance with the Policy on the Transmission of Protected Health Information and Personal Identifying Information.

UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Information Security Standards

Policy Statement

All University-owned or managed systems and information/data are assets of the University. These provisions apply to any systems or devices that store or process University-owned data regardless of whether the devices are owned or managed by the University or personally owned. Additionally, the encryption sections of this standard set forth the requirements for encrypting stored Protected Health Information (PHI) or Personal Identifying Information (PII) on UNC-Chapel Hill computing resources.

The security of these systems and information/data must be maintained according to the following Standards, which complement and supplement the Information Security Procedures.

Basic minimum requirements apply to all institutional information/data and systems and devices. More extensive requirements apply to Sensitive Information, particularly PHI and PII, and Mission-Critical Resources, as defined above.

All University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to campus ("Users") accessing the UNC network or UNC information through computing devices owned by or managed through UNC-Chapel Hill or through permission granted by UNC-Chapel Hill must read and adhere to these Standards.

Information Security Standards for Sensitive Information and Mission-Critical Resources

The following Standards apply to servers, workstations, laptops, and smartphones/PDAs that **do** store or process Sensitive Information or that **are** considered Mission Critical.

Please contact the ITS Helpdesk at 962-Help with any questions about how to implement these standards.

Standards Are Cumulative

The standards (requirements) described in the subsequent tables are cumulative, i.e., for a given device more than one of the subsequent tables may apply. For example, if a windows sever is storing Sensitive Information in a database, the server would be subject to the requirements for a windows server with Sensitive Information **AND** the database application standards.

"*" ITS provides IPS services.

Standards for Applications and Servers Storing or Processing Sensitive Information

In the following table, a "required" standard is indicated by an "X", and a "recommended" standard is indicated by an "R".

				Server	
	Mainframe	Web Applications	Database Applications	Windows	Unix/Linux/Mac
Security Controls					
Internet Filtering		X	X	X	X
Campus Filtering (from other UNC-CH hosts) [vlan or		X	X	X	X
Host-Based Firewall	X	X		R	R
Intrusion Prevention System*	X	X	X	X	X
Managed and Monitored Malware Protection				X	R
Detailed Auditing for Access to all Sensitive Files	X	X	X	X	X
Remote Copy of System Event Logs		X	X	X	X
24/7 Monitoring	X	X	X	X	X
Monthly Operating System Vulnerability Scans				X	X
Monthly Web Vulnerability Scans		X			
Monthly Database Vulnerability Scans			X		
Password Policy Enforcement	X	X	X	X	X
Two-Factor Authentication	R	R	R	R	R
Full-Disk Encryption					
Sensitive Field Encryption	R		X		
Encryption (File/Folder or Partition for all sensitive				R	R
Least Functionality	X	X	X	X	X
Least Privilege	X	X	X	X	X
Secure Backup (Encryption Recommended)	X	X	X	X	X
Incident Management Plan	X	X	X	X	X
Secure Physical Access	X	X	X	X	X
Patch Management (Automated Recommended)	X	X	X	X	X
VPN Software Installed					
Formal Admininistrator Security Training	X	X	X	X	X
Basic Security Awareness for End Users	X	X	X	X	X
Warning Banner for Services Requiring Authentication	X	X	X	X	X

Standards for Workstations, Laptops and Smartphones/PDAs Storing or Processing Sensitive Information

In the following table, a "required" standard is indicated by an "X", and a "recommended" standard is indicated by an "R".

	Workstation		Laptop		PDA
	Windows	Unix/Linux/Mac	Windows	Unix/Linux/Mac	
Security Controls					
Internet Filtering	R	R	R	R	
Campus Filtering (from other UNC-CH hosts) [vlan or fw]					
Host-Based Firewall	X	X	X	X	
Intrusion Prevention System*	X	X	R	R	
Managed and Monitored Malware Protection	X	R	X	R	R
Detailed Auditing for Access to all Sensitive Files	X	X	X	X	
Remote Copy of System Event Logs					
24/7 Monitoring	R	R			
Monthly Operating System Vulnerability Scans					
Monthly Web Vulnerability Scans					
Monthly Database Vulnerability Scans					
Password Policy Enforcement	X	X	X	X	X
Two-Factor Authentication	R	R	R	R	
Least Functionality	X	X	X	X	X
Least Privilege	X	X	X	X	
Secure Backup (Encryption Recommended)	R	R	R	R	
Incident Management Plan	X	X	X	X	X
Secure Physical Access	X	X	X	X	X
Patch Management (Automated Recommended)	X	X	X	X	X
VPN Software Installed			X	X	
Formal Admininistrator Security Training					
Basic Security Awareness for End Users	X	X	X	X	X
Warning Banner for Services Requiring Authentication					

Standards for Portable Media Devices Storing or Processing Sensitive Information[1]

In the following table, a "required" standard is indicated by an "X", and a "recommended" standard is indicated by an "R".

	Media		
	Tape Backup	CD/DVD	USB
Security Controls			
Internet Filtering			
Campus Filtering (from other UNC-CH hosts) [vlan or fw]			
Host-Based Firewall			
Intrusion Prevention System*			
Managed and Monitored Malware Protection			
Detailed Auditing for Access to all Sensitive Files			
Remote Copy of System Event Logs			
24/7 Monitoring	X		
Monthly Operating System Vulnerability Scans			
Monthly Web Vulnerability Scans			
Monthly Database Vulnerability Scans			
Password Policy Enforcement			
Two-Factor Authentication			
Least Functionality			
Least Privilege			
Secure Backup (Encryption Recommended)	X		
Incident Management Plan	X	X	X
Secure Physical Access	X	X	X
Patch Management (Automated Recommended)			
VPN Software Installed			
Formal Admininistrator Security Training	X		
Basic Security Awareness for End Users		X	X
Warning Banner for Services Requiring Authentication			

[1] Portable media devices include, for example, thumb drives, external hard drives, tape backup and optical medica.

Encryption Standards for Workstations, Laptops and Smartphones/PDAs Storing or Processing PHI or PII

In the following table, a “required” standard is indicated by an “X”, and a “recommended” standard is indicated by an “R”.

	Workstation		Laptop		Smartphone/PDA
	Windows	Unix/Linux/Mac	Windows	Unix/Linux/Mac	
Security Controls					
Full-Disk Encryption			X	R	R
Senstive Field Encryption					R
Encryption (File/Folder or Partion for all PHI or PII)	R	R	R	X	X

Encryption Standards for Portable Media Devices Storing or Processing PHI or PII

In the following table, a “required” standard is indicated by an “X”, and a “recommended” standard is indicated by an “R”.

		Media	
	Tape Backup	CD/DVD	USB
Security Controls			
Full-Disk Encryption			
Senstive Field Encryption			
Encryption (File/Folder or Partion for all PHI or PII)	X	X	X

Standards for Applications and Devices Considered Mission Critical

Devices such as workstations, smartphones, or PDAs are **not** included in the Mission Critical standards table since Mission Critical data should not be stored on any workstations or portable media devices.

In the following table, a "required" standard is indicated by an "X", and a "recommended" standard is indicated by an "R".

				Server	
	Mainframe	Web Applications	Database Applications	Windows	Unix/Linux/Mac
Security Controls					
Internet Filtering		X	X	X	X
Campus Filtering (from other UNC-CH hosts) [vlan or fw]		X	X	X	X
Host-Based Firewall	X	X	R	R	R
Intrusion Prevention System*	X	X	X	X	X
Managed and Monitored Malware Protection				X	R
Local System Event Logs	X	X	X	X	X
Remote Copy of System Event Logs		X	X	X	X
24/7 Monitoring	X	X	X	X	X
Monthly Operating System Vulnerability Scans				X	X
Monthly Web Vulnerability Scans		X			
Monthly Database Vulnerability Scans			X		
Password Policy Enforcement	X	X	X	X	X
Two-Factor Authentication	R	R	R	R	R
Network Access Control					
Least Functionality	X	X	X	X	X
Least Privilege	X	X	X	X	X
Secure Backup (Encryption Recommended)	X	X	X	X	X
Incident Management Plan	X	X	X	X	X
Secure Physical Access	X	X	X	X	X
Patch Management (Automated Recommended)	X	X	X	X	X
VPN Software Installed					
Formal Admininistrator Security Training	X	X	X	X	X
Basic Security Awareness for End Users	X	X	X	X	X
Warning Banner for Services Requiring Authentication	X	X	X	X	X
Cujo Entry				X	X

Minimum Standards for Non-Mission Critical Servers that Do Not Store Sensitive Information

The following tables describe the minimum security requirements for a server or any other device listed below to be connected to the UNC-Chapel Hill network. Unless one of the preceding standards apply regarding storage of Sensitive Information or Mission Critical status, any device connecting to the UNC-Chapel Hill network must meet, at a minimum, the following requirements before connecting to the network.

In the following table, a "required" standard is indicated by an "X", and a "recommended" standard is indicated by an "R".

	Windows	Unix/Linux/Mac
Security Controls		
Host-Based Firewall	R	R
Intrusion Prevention System*	X	X
Managed and Monitored Malware Protection	X	R
Detailed Auditing for Access	X	X
Password Policy Enforcement	X	X
Least Functionality	X	X
Least Privilege	X	X
Secure Backup (Encryption Recommended)	X	X
Incident Management Plan	X	X
Secure Physical Access	X	X
Patch Management (Automated Recommended)	X	X
Formal Admininistrator Security Training	R	R
Basic Security Awareness for Administrators	X	X
Warning Banner for Services Requiring Authentication	X	X

Minimum Standards for Non-Mission Critical Workstation, Laptop and Smartphone/PDA that Do Not Store Sensitive Information

In the following table, a "required" standard is indicated by an "X", and a "recommended" standard is indicated by an "R".

	Workstation		Laptop		PDA
	Windows	Unix/Linux/Mac	Windows	Unix/Linux/Mac	
Security Controls					
Host-Based Firewall	R	R	R	R	
Intrusion Prevention System*	X	X	R	R	
Managed and Monitored Malware Protection	X	R	X	R	R
Detailed Auditing for Access	R	R	R	R	
Password Policy Enforcement	X	X	X	X	X
Backup	R	R	R	R	
Incident Management Plan	X	X	X	X	X
Secure Physical Access	R	R	R	R	R
Patch Management (Automated Recommended)	X	X	X	X	X
VPN Software Installed for off-campus remote access			R	R	
Basic Security Awareness for End Users	R	R	R	R	R

Information Security Log retention requirements:

- Local System Event Logs and Remote Copy of System Event Logs: Logs, as related to Information Security events that describe who did what, when, where, and how, for devices storing Sensitive Information and Mission Critical systems, where technically feasible, must be maintained for ninety (90) days or 250 MB, whichever is more resource effective.

Contact Information

Subjects	Contact	Phone	Fax
Policy Questions Report a Violation Request Information Security Consulting	The University's Information Security Office	919-445-9393	919-445-9488

History

Effective Date:

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Revised Date: 6/30/10; __/__/11
Next Review Date: This policy will be reviewed at least annually.