UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Security Officer
Responsible Office
Information Security Office

STANDARD

UNC-Chapel Hill Information Security Controls Standard

Purpose and Background

This standard defines the minimum security controls for Information Technology systems in use at UNC-Chapel Hill. Units within the University may apply stricter controls to protect information and systems in their areas of responsibility. The standard applies to each UNC-Chapel Hill Affiliate for any covered system under their control.

Audience

All UNC-Chapel Hill Affiliates.

Standards

This Standard supersedes previous standards described in the UNC-Chapel Hill Information Security Policy dated 6/30/2010 and incorporates related guidance provided previously in other forms.

In order to comply with governing law, regulation, and policy at UNC-Chapel Hill while using information systems and associated technology, all users and administrators must implement at least the standards described here. Stricter standards may always be implemented at the discretion of departments.

The standards (requirements) described in the subsequent tables are cumulative, i.e., for a given device more than one of the subsequent columns may apply. For example, if a Windows server 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. These standards describe the minimum requirement. Stricter controls appropriate to the specific situation may be implemented as needed. Departmental standards may require stricter controls than the general University-wide standard described here.

In the charts below, notations are as follows:

1: Required item. Absent an approved exception, this control must be implemented.

2: Recommended item or best practice. This control should be implemented absent a technical obstacle or other compelling reason. If the control is not implemented, document any attempts to implement, rationale for not implementing, or other explanation.

- End user affiliates may consult their Information Security Liaison (ISL), help.unc.edu, or other campus resources for guidance, and must document any justification for non-implementation in writing only if asked.
- Justification for non-implementation of controls for server systems must be documented by systems administrators or department representatives via your ISL. (Documentation must be in place by May 1, 2016). Documentation should be stored in a secure location accessible to administrators and supervisors in the incident escalation path for the applicable system(s).

Blank (Shaded): Not applicable or optional. This control does not exist for the given category, does not apply, but security controls are always recommended if technically feasible.

MC: Mission Critical. The control applies differently to Mission Critical systems than to other systems in the same category.

SI: Sensitive Information. The control applies differently to systems that work with Sensitive Information than to other systems in the same category.

P/R: Protective/Reactive. Items listed as “P” are designed to protect systems or data, “R” items are controls which aid in responding to an incident or system issue.

See descriptions of controls following the tables.

Servers

KEY: Security Controls: **1**=Required; **2**=Recommended; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information; **P/R** = Protective/Reactive.	Note	Mainframe	Web Applications	Database Applications	Windows Servers	Unix/Linux Servers
Internet Filtering [special router ACLs or campus firewall]	P	1	1	1	1 (2 if no SI or MC)	1 (2 if no SI or MC)
Campus Filtering (from other UNC -CH hosts) [vlan ACLs or firewall]	P		1	1	1	1
Host-Based Firewall	P	1	1	1	1	1
Intrusion Prevention System	P	1	1	1	1	1
Managed and Monitored Malware Protection	PR				1	2
Detailed Auditing for Access (account access)	R				2	2
Detailed Auditing for Access to all Sensitive Files (file access)	R	2	2	2	2	2
Local System Event Logs	R		2	2	2	2
Remote Copy of System Event Logs	R		2	2	1 (2 if no SI or MC)	1 (2 if no SI or MC)
24/7 Monitoring	R	1	1 (2 if not MC)	1 (2 if not MC)	1 (2 if not SI or MC)	1 (2 if not SI or MC)
Operating System Vulnerability Scans (Authenticated)	P, R				1 if SI or MC	1 if SI or MC
Web Vulnerability Scans	P, R		2			
Database Vulnerability Scans	P, R			2		
Password Policy Enforcement (User and Administrator)	P	1	1	1	1	1
Multi-Factor Authentication	P	2	2	2	2 if SI or MC	2 if SI or MC
Sensitive Field Encryption	P	2		2		
Encryption (File/Folder or Partition for all SI)	P				2	2
Least Functionality (refers to services and device purpose)	P	1	1	1	1	1
Least Privilege (refers to user accounts, service accounts, and processes)	P	1	1	1	1	1
Backup/Archive	P, R	1	2	2	2	2
Secure Physical Access	P	1	1	1	1	1
Patch Management (Automated Recommended)	P, R	1	1	1	1	1
Formal System Administration Initiative Training	P		1	1	1 if SI or MC	1 if SI or MC
ITS Security Awareness for End Users (or Equivalent)	P	1			1	1
Warning Banner for Services Requiring Authentication	P	1	2	2	2	2
System Contact	R				1 if SI or MC	1 if SI or MC
Risk Assessment	P		1 if MC or SI	1 if MC or SI	1 if MC or SI	1 if MC or SI
Vendor-Supported Operating System	P		1	1	1	1
Register system with System Administration Initiative (SAI)	P		1 if SI or MC	1 if SI or MC	1 if SI or MC	1 if SI or MC
Vendor-Supported Applications	P		2	2	2	2

Workstations and Mobile Devices

KEY: Security Controls: **1**=Required; **2**=Recommended; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information; **P/R** = Protective/Reactive.	Note	Windows Workstation	Unix/Linux/ Mac Workstation	Windows Laptop	Unix/Linux /Mac Laptop	Other Mobile Device (incl Smartphone)
Internet Filtering [special router ACLs or campus firewall]	P	2	2	2	2	
Campus Filtering (from other UNC -CH hosts) [vlan ACLs or firewall]	P	1 if SI	1 if SI	1 if SI	1 if SI	
Host-Based Firewall	P	1	1	1	1	
Intrusion Prevention System	P	1 (2 if not campus)	1 (2 if not campus)	1 (2 if not campus)	1 (2 if not campus)	
Managed and Monitored Malware Protection	P	1	2	1	2	2
Detailed Auditing for Access	R	2	2	2	2	
Detailed Auditing for Access to all Sensitive Files	R	2	2	2	2	
Local system event logs	R	2	2	2	2	
Operating System Vulnerability Scans (Authenticated)	P, R,	2 if SI or MC	2 if SI or MC	2 if SI or MC	2 if SI or MC	
Password Policy Enforcement (User and Administrator)	P	1	1	1	1	2
Full-Disk Encryption	P	2 if PHI/PII	2 if PHI/PII	1 If PHI/PII	1 if PHI/PII	2 if PHI/PII
Encryption (File/Folder or Partition for all SI)	P	2	2	2	2	2
Least Functionality (refers to services and device purpose)	P	2	2	2	2	2
Least Privilege	P	1 if SI	1 if SI	1 if SI	1 if SI	2 if SI
Backup/Archive	P, R,	2	2	2	2	
Secure Physical Access	P	2	2	2	2	2
Patch Management (Automated Recommended)	P, R,	1	1	1	1	1
VPN Software for remote access	P	1(2 if no SI)	1 (2 if no SI)	1(2 if no SI)	1(2 if no SI)	2 if SI
ITS Security Awareness Training for End Users (or Equivalent)	P	1	1	1	1	1
Warning Banner for Services Requiring Authentication	P	2	2	2	2	
Vendor-Supported Operating System	P	1	1	1	1	1if SI
Vendor-Supported Applications	P	2	2	2	2	

User-owned workstation or laptop devices are held to the same control standards when used for University business purposes. Each owner is responsible for securing their device(s). University operating units may opt to provide assistance or compensating controls to assist the user to comply with or to obtain exception for burdensome or technically challenging controls.

Media

KEY: Security Controls: **1**=Required; **2**=Recommended; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information; **P/R** = Protective/Reactive.	Note	Tape Media	Optical Media	Portable drive
Full-Disk Encryption	P	2 PHI/PII		2 PHI/PII
Encryption (File/Folder or Partition)	P	1 PHI/PII	1 PHI/PII	1 PHI/PII
Secure Physical Access	P	1	2	2

Control Descriptions (See Charts above)

24/7 Monitoring: Automated monitoring for system state (up or down) with notification escalations for state changes.

Backup/Archive: Information assets of the University must be preserved via a backup which can be restored. Testing of backups to ensure viability should be performed periodically. Backup may be full or partial as appropriate so long as the University information assets on the system can be restored.

Campus Filtering: Network segmentation from other UNC-Chapel Hill hosts through the use of VLAN access control lists (ACLs) or firewall.

Detailed Auditing for Access: Detailed audit logs that document electronic access to Sensitive Information, should be stored for the duration specified in any applicable records retention policy, but generally retained for 90 days or 250MB. Logs should be periodically reviewed or alerts set on logged information to detect any unauthorized access.

Encryption (File/Folder or Partition for all PHI/PII): Encoding a specific file/folder or partition that contains protected health information (PHI) or personally identifiable information (PII) in such a way that only an authorized individual/system can read it.

Formal System Administrator Initiative (SAI) Training: The SAI course offered by ITS via the Sakai Learning Management System. This course is required for anyone on campus who has elevated privileges on a server which allow that user to perform such tasks as modifying system configuration settings or administering user access.

Full-Disk Encryption: The automatic conversion of data on an entire hard drive or comparable storage medium into a format which cannot be understood by anyone who does not have the key to decrypt, or “undo” the conversion. Encryption must be implemented according to current best practices. An application that automatically encrypts all non-OS files without user interaction satisfies the requirement for full-disk encryption. For media (tape, disk) if full-disk encryption is used, then file/partition encryption is optional. Full-Disk Encryption is only required for those systems storing

Sensitive Information. NOTE: Some systems may cache information they process in files that may stay on the system.

Host-based Firewall: Software firewall running on a single host that can restrict incoming and outgoing network traffic for that host only.

Internet Filtering: Network segmentation from the Internet (non-campus network) through the use of special router access control lists (ACLs) or the campus firewall.

Intrusion Prevention System (IPS): Network security appliances that monitor network and/or system activities by identifying malicious activity, logging information about this activity, attempting to block/stop it, and reporting it.

ITS Security Awareness Training for End Users (or equivalent): End users of University systems must have completed the Basic Security Awareness for End Users course. All users with an Onyen must complete the training annually.

Least Functionality: The information system is configured to provide only essential capabilities and specifically prohibits unnecessary and/or non-secure functions, ports, protocols, and services. Examples may include, but are not limited to: Trivial File Transfer Protocol (TFTP) and peer-to-peer file sharing protocols such as BitTorrent.

Least Privilege: Users (including application and system accounts) of these systems should only be able to access the information and resources that are necessary to perform their jobs.

Local System Event Logs: Event logs are special files that record significant events on a computer, such as when a user logs on or when a program encounters an error. Detailed audit logs must document electronic access to Sensitive Information should be stored for the duration specified in any applicable records retention policy, but generally retained for 90 days or 250MB. Logs should be periodically reviewed or alerts set on logged information.

Managed and Monitored Malware Protection: Malware protection solutions (anti-malware) that are both in a managed and monitored state by a centralized IT unit having alerting and reporting capabilities. If not possible to automate, there must be justification

for the non-compliance and all users of non-automated systems must be told to immediately report any notification from their host-based application.

Multi-factor Authentication: Security configuration which requires multiple methods of authentication from the following categories:

- "Something you have" (i.e. RSA token),
- "Something you know" (i.e. PIN or a password)
- "Something you are" (i.e. biometric data such as fingerprints, retinal scan)

Multi-factor is recommended for all privileged accounts.

Password Policy Enforcement: Enforcement of the UNC-Chapel Hill Password Policies for General Users, System and Application Administrators.

Patch Management: The frequency and prioritization of the installation of patches to computer systems. Patch application follows existing policy, including the Vulnerability Management Policy.

Remote Copy of System Event Logs: Replication of system event logs to syslog or other Security Information and Event Management (SIEM) system for improved aggregation, correlation, alerting and reporting activities.

Risk Assessments: Any information system that creates, receives, maintains, or transmits University-owned sensitive information must have a thorough and timely risk assessment of the potential threats and vulnerabilities to the confidentiality, integrity, and availability *before the purchase or integration of new technologies and/or changes in the architecture of an existing system that may impact security controls*. (This control does not apply to existing systems until architecture changes are planned or a periodic evaluation is required. See below.) Based on the outcome of a Risk Assessment, risk mitigation activities may be required which would include developing a strategy agreed-upon by the Chief Information Security Officer (CISO) and the relevant stakeholders to efficiently and effectively mitigate the identified risks in the assessment process or document any acceptance of identified risks. HIPAA risk analysis for information systems containing electronic protected health information (ePHI) will be conducted on a periodic basis. If the time required to perform a risk assessment would significantly impact organizational mission, the department and data steward may appeal to the Office of the CIO or delegate.

Secure Physical Access: Implement a set of measures, appropriate to the system to ensure that the ability of people to physically gain access to a computer system is restricted to authorized users. Specific strategies include, but are not limited to the use of: Badge access controls and logging for areas containing critical or sensitive resources, fire detection and suppression mechanisms, temperature and humidity controls, emergency lighting, water damage protection, emergency power and shutoff mechanisms, protection of screens which may display sensitive information. Installation in an access-controlled area, logs to record entries to the secure area, positioning systems to minimize unauthorized viewing of Sensitive Information.

Sensitive Field Encryption: Also known as application-level encryption, performs the encryption/decryption process within the application that generates the data stored in the database. The benefit of this method is the separation of the encryption keys, kept on the application server, from the encrypted data in the database. The application must be developed to support this functionality."

System Contact: The ITS Control Center houses contact information (both "Business Day," and "Off Hours") for registered hosts. The information is to be used in the event of an incident involving that host. Contact information and escalation record information must be provided to the Control Center via help ticket and kept up-to-date for each host.

Vendor-Supported Application: The application vendor must still be publishing security patches for the application version in use.

Vendor-Supported Operating System: The Operating System vendor must still be publishing security patches for the OS version in use.

VPN Software Installed: System employs VPN software provided or approved by ITS Network Services for remote connections over unsecure networks.

Vulnerability Scan (Operating System, Web, Database) : Vulnerability scans that are run with administrator/root-level access at least on a monthly basis on the operating system. Scanning may be done every six months for web applications, and if a risk-assessed web-application firewall is in use, then annual scan is acceptable. Database applications residing behind network firewalls, and using a host-based firewall may scan every six months. Workstations/Laptops: Those residing behind a University firewall, with host-

based firewall enabled, and attached to the Active Directory domain may scan annually rather than monthly. Vulnerability scanning is only required for those workstations and laptops storing Sensitive Information, not for those systems merely accessing the information. NOTE: Some systems may cache information they process in files that may stay on the system.

Warning Banner for services requiring authentication: An approved system use notification message is displayed on a computer screen prior to allowing the user to access the system. The message includes privacy and security notices consistent with any applicable federal or state laws, university directives, policies, or other guidance and at minimum notifies users that:

- Unauthorized access may result in penalties
- The System is a UNC system
- Any responsibilities the user may have for use of the system

Exceptions to the Standard

The heterogeneous nature of the UNC-Chapel Hill computing environment is such that in many cases a specific business unit will have unique technology requirements, and will use compensating controls to achieve appropriate security risk management. This exception process is intended to provide for the unit, any involved Data Steward, and the ISO to work collaboratively to document appropriate security controls for challenging environments. In most cases, unit staff will be the subject matter experts for appliances, single-purpose systems, and for their own business requirements. The ISO has the ultimate responsibility for University Information Security practices, and expertise on security practices. When a unit requires a control exception, and brings good background information and requirements into the process, an open communication process should result in a well-documented exception.

Process

Exceptions may be submitted for approval by the CISO or delegate via help ticket. Exceptions may be requested on a device-by-device basis, or with a single request covering multiple identical devices with the same basis for exception (“Exemplars”), or with a single request covering a system of devices which use the same set of compensating controls.

Exception review shall include consideration of: Compensating controls in place, impact on organizational mission, any recommendations from campus resources related to a specific vulnerability or specific system's remediation, technical obstacles to remediation, operational obstacles to remediation, any other environment-specific information provided in the request. Generally speaking, cost to remediate must be prohibitive to the department and the appropriate data steward must sign off in order for an exception to be considered.

During review of the exception request by the CISO or delegate, remediation timelines would likely be extended, depending on risk to the University and at the discretion of the CISO. Any such extension must be authorized in writing.

If an exception is not granted, the department may appeal the denial to the CIO; the CIO may request involvement of the affected Department Head. If the result of non-remediation would be removal of the system from the network or other high-impact action, the CISO shall seek approval of the CIO to take such action.

Approved Blanket Exceptions

Encryption is not required for laptops that are accessing sensitive information exclusively through an ISO-approved secured Virtual Desktop Interface (VDI) (e.g., CITRIX or other approved VDI).

Compliance

Failure to comply with this standard 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 standard may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this standard may face termination of their business relationships with UNC-Chapel Hill.

Violation of this standard may also carry the risk of civil or criminal penalties.

Definitions

Covered System: Computing device used for University Business.

Information Security Office (ISO) Risk Assessment: The process of identifying, prioritizing, and estimating risks. Incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Mission Critical: A system so critical to the mission of the UNC-Chapel Hill business unit that any incident requires immediate response. If a system is deemed mission critical by the department, then contact and escalation information has been provided for the system in advance of any incident or outage. The owning business unit determines whether a resource is mission critical. Once designated as mission critical, heightened information security policies and standards apply in an effort to assure that the resource remains available. If a business unit does not designate a resource as mission critical, that resource may not be a priority for restoration of services in the event of an incident or outage.

Sensitive Information: Systems within scope for control of Sensitive Information are those storing information which may pose a risk of harm to the University if disclosed in an unauthorized manner. This includes information which the University is required by law, regulation, contract, policy, or other governing requirement to keep confidential. NOTE: Some systems may cache information they process in files that may stay on the system.

UNC-Chapel Hill Affiliate: UNC-Chapel Hill faculty, staff, students, retirees, contractors, distance learners, visiting scholars and others who require UNC-Chapel Hill resources to work in conjunction with UNC-Chapel Hill.

Related Documents

Information Security Policy

End User Security Training

UNC Help & Support: What is Sensitive Information, UNC Help & Support: Securing Sensitive Information and UNC Help & Support: Examples of Sensitive Information

Contacts

Subject	Contact	Telephone	Online
Standards Interpretation or Assistance With Controls	UNC ITS Information Security Office	919-962-HELP	help.unc.edu

Document History

- Effective Date and title of Approver: (Prior document, Information Security Policy authorized 3/6/2010, Chief Information Officer)
- Revision and Review Dates
  - Revised: 6/30/2011
  - Revised: 1/20/2016
- Change notes: The standards contained in this document were previously laid out in the Information Security Controls Policy. These standards were moved into their own document superseding all related controls sections of the Information Security Controls Policy.