THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Issuing Office(s)
Information Technology Services

Responsible University Officer(s)
Chief Information Security Officer

UNIVERSITY STANDARD

Title

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL INFORMATION SECURITY CONTROLS STANDARD

Introduction

PURPOSE

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.

SCOPE OF APPLICABILITY

All UNC-Chapel Hill Constituents and units.

Standard

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. Additional controls are implemented at the University level, individual users do not have responsibility for implementing these controls.

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:

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

B: Recommended item. 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 users 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 before the system goes into Production or contains any Tier 2 or 3 information). Documentation should be stored in a secure location accessible to administrators and supervisors in the incident escalation path for the applicable system(s).

C: Advisory item. This control should be evaluated for implementation where appropriate.

Blank (Shaded): Not applicable or optional. This control does not exist for the given category or does not apply. Appropriate 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. Refers to information type 2 or 3 in the Information Security Classification Standard. 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.

SECURITY CONTROLS

Servers

KEY: Security Controls: **A**=Required; **B**=Recommended; C= Advisory; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information Tier 2/3; **P/R** = Protective/Reactive.	Note	Web Applications	Database Applications	Windows Servers	Unix/Linux Servers
Internet Filtering (special router ACLs or campus firewall)	P	A	A	A (B if no SI or MC)	A (B if no SI or MC)
Host-Based Firewall	P	A	A	A	A
Intrusion Prevention System	P	B	B	B	B
Managed and Monitored Malware Protection	PR			A	B
Detailed Auditing for Access (account access)	R			B	B
Detailed Auditing for Access to all Sensitive Files (file access)	R	A for PHI, B for Tier 3	A for PHI, B for Tier 3	A for PHI, B for Tier 3	A for PHI, B for Tier 3
Local System Event Logs	R	B	B	B	B
Remote Copy of System Event Logs	R	B	B	A (B if no SI or MC)	A (B if no SI or MC)
24/7 Monitoring	R	B	B	A (B if not SI or MC)	A (B if not SI or MC)
Operating System Vulnerability Scans (Authenticated)	P, R			A if SI or MC	A if SI or MC
Monthly Web Vulnerability Scans	P, R	B			
Monthly Database Vulnerability Scans	P, R		B		
Password Policy Enforcement (User and Administrator)	P	A	A	A	A
2-Step Verification or Multi-Factor Authentication	P	B	B	B	B
Sensitive Field Encryption	P		B		
Encryption (File/Folder or Partition for all SI)	P			B	B
Least Functionality (refers to services and device purpose)	P	A	A	A	A
Least Privilege (refers to user accounts, service accounts, and processes)	P	A	A	A	A
Backup/Archive	P, R	B	B	B	B

KEY: Security Controls: **A**=Required; **B**=Recommended; C= Advisory; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information Tier 2/3; **P/R** = Protective/Reactive.	Note	Web Applications	Database Applications	Windows Servers	Unix/Linux Servers
Secure Physical Access	P	A	A	A	A
Patch Management (Automated Recommended)	P, R	A	A	A	A
Formal System Administration Initiative Training	P	A	A	A	A
ITS Security Awareness for End Users (or Equivalent)	P	C	A	A	A
Warning Banner for Services Requiring Authentication	P	B	B	B	B
System Contact	R			A if SI or MC	A if SI or MC
Risk Assessment	P	A if MC or SI	A if MC or SI	A if MC or SI	A if MC or SI
Vendor-Supported Operating System	P	A	A	A	A
Register system with System Administration Initiative (SAI)	P	A if SI or MC	A if SI or MC	A if SI or MC	A if SI or MC
Vendor-Supported Applications	P	B	B	B	B
Application timeout	P	C	C		
Secure Configuration	P			B	B
Onyen Authentication	P			C	C
Shibboleth Authentication	P	C			
Input/Output Validation	P	C			
Account Lock-Out	P	B	B	B	B
Network Session Timeout	P	B	B		

Workstations and Mobile Devices

KEY: Security Controls: **A**=Required; **B**=Recommended; C= Advisory; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information Tier 2/3; **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	B	B	B	B	
Host-Based Firewall	P	A	A	A	A	
Managed and Monitored Malware Protection	P	A	B	A	B	B
Detailed Auditing for Access (Account Access)	R	B	B	B	B	
Detailed Auditing for Access to all Sensitive Files (File Access)	R	A for PHI B for Tier 3 C for Tier 2	A for PHI B for Tier 3 C for Tier 2	A for PHI B for Tier 3 C for Tier 2	A for PHI B for Tier 3 C for Tier 2	
Local system event logs	R	B	B	B	B	
Operating System Vulnerability Scans (Authenticated)	P, R,	A if Tier 2 or 3 or MC	A if Tier 2 or 3 or MC	B if Tier 2 or 3 or MC	B if Tier 2 or 3 or MC	
Password Policy Enforcement (User and Administrator)	P	A	A	A	A	B
Full-Disk Encryption	P	B if PHI/PII or Tier 3	B if PHI/PII or Tier 3	A If PHI/PII or Tier 3	Bif PHI/PII or Tier 3	B if PHI/PII or Tier 3
Encryption (File/Folder or Partition for all SI)	P	B	B	B	B	B
Least Functionality (refers to services and device purpose)	P	B	B	B	B	B
Least Privilege (refers to user accounts, service accounts, and processes)	P	B if Tier 2 or 3	B if Tier 2 or 3	B if Tier 2 or 3	B if Tier 2 or 3	B if Tier 2 or 3

KEY: Security Controls: **A**=Required; **B**=Recommended; C= Advisory; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information Tier 2/3; **P/R** = Protective/Reactive.	Note	Windows Workstation	Unix/Linux/ Mac Workstation	Windows Laptop	Unix/Linux /Mac Laptop	Other Mobile Device (incl Smartphone)
Backup/Archive	P, R,	B	B	B	B	
Secure Physical Access	P	B	B	B	B	B
Patch Management (Automated Recommended)	P, R,	A	A	A	A	A
VPN Software for remote access	P	A(B if no SI)	A (B if no SI)	A(B if no SI)	A(B if no SI)	B if SI
ITS Security Awareness Training for End Users (or Equivalent)	P	A	A	A	A	A
Warning Banner for Services Requiring Authentication	P	B	B	B	B	
Vendor-Supported Operating System	P	A	A	A	A	A if SI
Vendor-Supported Applications	P	B	B	B	B	
Secure Configuration	P	B	B	B	B	
Onyen Authentication	P	C	C	C	C	
Secure Disposal	P	A if Tier 2 or 3	A if Tier 2 or 3	A if Tier 2 or 3	A if Tier 2 or 3	A if Tier 2 or 3
Account Lock-Out	P	C	C	C	C	C
Screen-Lock	P	B	B	B	B	B if Tier 2 or 3

User-owned workstation or laptop devices are held to the same control standards when used for University 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.

Data

Security controls are largely intended for the purpose of protecting University Data (as well as technology assets). The following controls apply regardless of where University data resides. When addressing "recommended" controls, resources should be prioritized to protect Tier 3 data (more sensitive data) over less sensitive data.

For Sensitive (Tier 2 or 3) Data, follow posted University storage guidelines regarding approved locations.

Media

KEY: Security Controls: **A**=Required; **B**=Recommended; C= Advisory; **Blank**=N/A or Optional; **MC** = Mission Critical; **SI** = Sensitive Information Tier 2/3; **P/R** = Protective/Reactive.	Note	Tape Media	Optical Media	Portable drive
Full-Disk Encryption	P	B PHI/PII or Tier 3, B if Tier 2		A if PHI/PII or Tier 3, B if Tier 2
Encryption (File/Folder or Partition)	P	A PHI/PII	A PHI/PII	A PHI/PII
Secure Physical Access	P	A	B	B
Secure Disposal	P	A if Tier 2 or 3	A if Tier 2 or 3	A if Tier 2 or 3

Control Descriptions (See Charts above)

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

2-Step Verification or 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.

Account Lock-out: After 10 failed attempts to long-in, the application or information system will deny new access for the user account for a period of at least 5 minutes. After 5 minutes the user account may be unlocked. (It is permissible to configure systems to discount use of a recent password for the purposes of counting failed log-in attempts.)

Application Time-out: Application owners should determine an appropriate time-out based on the risks, specific constraints, and environment of the system.

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. Please consult your local IT support for workstation backup options.

Campus Filtering: Network segmentation from other UNC-Chapel Hill hosts through the use of VLAN access control lists (ACLs) or firewall. (This control is implemented by the University. Please contact your local IT support if you have questions)

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. Note, additional requirements may be required for specific types of systems, including those containing protected health information (PHI). Adhere to longer duration retention if required.

Encryption (File/Folder or Partition): 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. For media (tape, disk) if full-disk encryption is used, then file/partition encryption is optional.

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. 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. When host-based firewall is not technically feasible, VLAN ACLs or network firewall may be implemented as alternatives.

Input/Output Validation: Use of proper coding techniques for web applications to prevent attackers from inserting malicious commands.

Internet Filtering (Special router ACLs or Campus Firewall): Network segmentation from the Internet (non-campus network) through the use of special router access control lists (ACLs) or the campus firewall. (ITS provides this filtering for systems on University networks. Individual users or administrators are responsible for ensuring this control is in place on off-campus systems. Please contact your local IT admin if you have questions.)

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. (The University implements various Intrusion Prevention Systems on campus networks. Please contact your local IT admin if you have questions.)

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 Admin privileges must be allowed only on an as-needed basis.

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 or as required for regulatory compliance (including HIPAA compliance), 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. Users of non-automated systems can comply with this control by immediately reporting any notification from their host-based application. (The University implements various Malware Protection Systems on campus networks. Please contact your local IT admin if you have questions.)

Network Session Timeout: An application or information system should terminate an existing connection/session after a period of inactivity lasting more than 15 hours.

Onyen Authentication: Systems should use Onyen Authentication if technically feasible. See references below for service information.

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

Patch Management (Automated Recommended): 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, and to protect the logs from malicious tampering.

Risk Assessment: Any information system that creates, receives, maintains, or transmits University-owned or managed sensitive information must have a risk assessment of the potential threats and vulnerabilities to the confidentiality, integrity, and availability before sensitive data is loaded or mission-critical functions are in production. (This control does not apply to existing systems until architecture changes or addition of higher-tier data are planned or a periodic evaluation is required based on a risk determination by or at the request of the CISO.) Based on the outcome of a Risk Assessment, risk mitigation activities may be required by the Chief Information Security Officer (CISO) and/or the relevant stakeholders. 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/or data steward may appeal to the Office of the CIO or delegate. The Information Security Office may determine the scope of any risk assessment or that a risk assessment is not required or may be deferred. NOTE: Independent third-party assessments or other alternate assessments will be considered by the ITS at the request of a department such as Service Organization Controls (SOC) 2, Type 2. These may significantly reduce the time required for an assessment.

Screen-lock: Each user login will be locked out automatically after 30 minutes of inactivity. (30 minutes is the longest permissible duration of inactivity before lock-out. Implementation of shorter duration lock-out controls is acceptable).

Secure Configuration: When installing and configuring operating system and applications, do so using best practices to disable unused ports or other means of access, change default passwords, and make other configuration decisions that will reduce risk while maintaining needed functionality. Guidance from NIST on secure configuration is available here: https://web.nvd.nist.gov/view/ncp/repository

Secure Disposal: Disposal procedures depend upon the type and intended disposition of media (reuse, repair, replacement, removal). All storage media in systems covered by this Standard must be properly sanitized before it is transferred from the custody of its current owner. (Transfer within the same business unit without sanitization is permissible if appropriate precautions, such as drive formatting, are taken to ensure that no unauthorized person can access data by ordinary means). The proper sanitization method depends on the type of media and the intended disposition of the media. Sanitization may be accomplished by overwriting or destruction of the media.

Overwriting requires three overwriting passes and a verification pass. A variety of software packages are available on the open market that properly perform this function. Examples of software programs that can be used to overwrite media include Pretty Good Privacy, Eraser, and KillDisk. Destruction requires damaging the media to make it unusable by any device that may normally be used to read information on the medium. University units must maintain documentation of sanitization of hard drives. Equipment designated for surplus or other re-use should have a label affixed stating that the hard drive has been properly sanitized. Equipment transferred to a third party for repair or data recovery is permissible if the third-party has an agreement in place with the University to properly address data management (ex: Business Associate Agreement if PHI is on the device).

Original drives must be disposed of securely according to this Standard. Damaged or inoperable media that cannot be overwritten must be destroyed. Secure shredding of drives is available from the UNC Surplus Property warehouse (919-962-2134). Additional guidance is available here: http://help.unc.edu/help/electronic-media-disposal-faq/

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 key management) 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 workstations should not be located in lobbies or other lightly-secured areas without additional controls such as cable, encryption, etc.

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."

Shibboleth Authentication: Systems and applications should use Shibboleth, integrating with the Web Single-Sign-On (SSO) solution provided by ITS ID Management, if technically feasible. See references below for service information.

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. If patches are available from an alternate source, such as an open-source community or in-house developer, that satisfies this control.

Vendor-Supported Operating System: The Operating System vendor must still be publishing security patches for the OS version in use. If patches are available from an alternate source, such as an open-source community or in-house developer, that satisfies this control.

VPN Software for Remote Access: System employs VPN software provided or approved by ITS Network Services for remote connections over unsecure networks. Intended for off-campus workstations accessing sensitive information.

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 (Web application scans need not be run with administrator permissions). 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.

Alternative controls to Web and Database vulnerability scans may be implemented with documented justification. 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

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 requests a control exception, and provides good background information and justifications, an open communication process can result in a well-documented exception.

Process

Exceptions may be submitted for approval to 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, cost to remediate must be prohibitive to the department if used as justification for the exception request. The appropriate data steward must provide approval of the request 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).

Security controls that cannot be feasibly applied as-written for cloud services may be omitted under some circumstances. Follow ISO guidance regarding storage of sensitive information in Office 365 and other cloud vendors (see references below).

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: Information classified as Tier 2 or Tier 3 in the UNC-Chapel Hill Information Classification Standard.

University Constituent: UNC-Chapel Hill faculty, staff, students, retirees and other affiliates, contractors, distance learners, visiting scholars and others who use or access UNC-Chapel Hill resources.

Related Requirements

EXTERNAL REGULATIONS AND CONSEQUENCES

Health Insurance Portability and Accountability Act (HIPAA)
Family Educational Rights and Privacy Act (FERPA)
North Carolina Identity Theft Protection Act (NCID)
NC Public Records, NCGS Chapter 132

COMPLIANCE

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

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

UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES

Information Security Policy

End User Security Training

Office 365 Data Sharing Guidance

See available Malware protection packages

Web Single-Sign-On

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

Contact Information

PRIMARY CONTACT(S)

1. UNC ITS Information Security Office
   Title: Information Security Office
   Unit: ITS
   Email: help.unc.edu
   Phone: 919-962-HELP

OTHER CONTACTS

ITS Policy Office: its_policy@unc.edu

Important Dates

- Effective Date and title of Approver: (Prior document, Information Security Policy)
  a. Effective Date: 3/6/2010
  b. Approver: Chief Information Officer

  a. Revised Date: 6/30/2011
  b. Revised by: Chief Information Officer
  c. Substantive Revisions: Unknown

  a. Effective Date: 1/20/2016 (Information Security Controls Standard)
  b. Approver: Chief Information Security Officer
  c. Substantive Revisions: 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.

- Revision and Review Dates, Change notes, title of Reviewer or Approver:

  a. Last Revised: 10/25/2017
  b. Revised by: Chief Information Security Officer
  c. Substantive Revisions: Incorporating Electronic Media Disposal (superseding existing Electronic Media Disposal Standard), adding application and network session timeout controls, removing mainframe controls, altering Risk Assessment control, addition of “advisory” items, added data classification tiers for some controls, language clarifications throughout. Adjustments to control levels throughout.