University Standard on Information Technology Access Control

**Introduction**

**PURPOSE**

To guide University Constituents in preserving the integrity, confidentiality, and availability of University information and information systems. Access controls are intended to minimize inappropriate exposure of University information by limiting system access to authorized individuals.

**SCOPE OF APPLICABILITY**

University Constituents and units responsible for management of IT systems or University Enterprise Data.

**ACCESS RIGHTS MANAGEMENT**

Access to multi-user systems containing University data must be authorized.

Requests for privileged access authorization must be made according to established processes for each system and be based on business or academic need for the access. Authorization for access to mission critical systems or those containing Tier 2 or 3 (sensitive) information must be revoked when an individual's change in employment status, job function, or responsibilities no longer requires specialized access privileges. Authorization of access to non-privileged accounts may be based on user role/group rather than individual authorization.

**ACCESS CONTROLS**

Access controls should be appropriate to the sensitivity of the data as outlined in the Information Security Control Standard.

Mechanisms to control access to Mission-Critical Devices and those containing information classed as Tier 2 or Tier 3 (Sensitive Information) must include at a minimum the following methods:
Authorization

All additions, changes, and deletions to individual access must be approved by the individual(s) responsible for management of each system's access and must have a valid business justification. For example, access to an administrative system may require approval by a user's supervisor, an Access Request Coordinator, and the Data Steward (or Manager/Custodian) with authority to grant access to the specific data requested. Authorized account creation, deletion, and modification as well as access to protected data and network resources is completed by the unit responsible for technical management or security of the system or units with delegated authorization to manage the system.

Administrative and system technical support account authorization must be approved by (at a minimum) the individual(s) responsible for technical management of the system. This may be an IT Guardian or their delegate. Every system and service account must have a designated responsible individual. If that individual changes, a new individual must be designated.

Individuals may not authorize their own access unless an exception applies.

Identification and Authentication

Unique user identification (User ID) and authentication is required by the UNC-Chapel Hill Information Security Controls Standard. All users of subject systems must adhere to applicable IT policies related to User ID's, including provisions related to maintaining the integrity of access credentials. Those responsible for implementation of this standard must act to enforce those policies and standards by holding Users accountable for noncompliance.

For detailed standards, consult the Information Security Control Standards and the Policy on the Transmission of Sensitive Information.

Third Party Access

All third-party access to multi-user systems must be approved by the individual responsible for technical oversight of that system, and the appropriate business data representative.

Third parties may have administrative/privileged access to University systems only with an appropriate business justification and authorization for each affected system.

All third-party accounts on systems considered Mission Critical or those containing Tier 2 or 3 information will be disabled and inactive unless needed for support or maintenance. The technical staff responsible for system management will be responsible for enabling/disabling accounts and monitoring vendor access to said systems.

All third parties with access to any considered Mission Critical or those containing Tier 2 or 3 information must adhere to all regulations and governance standards associated with that data (e.g. PCI security requirements for cardholder data, FERPA requirements for student records, HIPAA for protected health information (PHI), University Committee for the Protection of Personal Data (UCPPD) for SSNs). Third party accounts must be immediately disabled after support or maintenance is complete.

Remote Access

All remote access to systems containing University Enterprise Data classed as Tier 2 or 3 (sensitive information) or those designated as Mission Critical must be authenticated and encrypted According to the
Physical Access

Multi-user Mission-Critical computer systems and those containing information classed as Tier 2 or 3 (sensitive information) and the infrastructure required to support them must be installed in an access-controlled area in accordance with the UNC-Chapel Hill Information Security Control Standards. This includes protecting such devices from physical access by unauthorized individuals.

Procedures or processes must be implemented to regularly audit users granted access to each area and to remove assignment based on changes in roles or responsibilities.

Sensitive information must not be stored on mobile devices or disposable media devices without compliance with the Information Security Control Standards including protecting such devices from physical access by unauthorized individuals.

ACCESS AUDIT AND REVIEW

Units and Constituents responsible for access-controlled systems must create and follow documented Processes or procedures to regularly review individual and system account access to such systems. This includes review of all physical (badge) access granted.

Access review is only required for systems with Tier 2 or 3 data and mission critical systems.

Individuals responsible for access control for each system must review and approve all requests for access modifications. Their responsibilities under this standard include:

- 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 when access is no longer necessary or appropriate.
- Reporting promptly 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 and Incident Management Policy.
- Initiating appropriate actions when Information Security Incidents are identified in accordance with the Incident Management Policy.

EXCEPTIONS

Exceptions to this Standard may be made by the Vice Chancellor for Information Technology and Chief Information Officer (CIO or their delegate(s), authorized in writing.

Access roles only permitting users to access to their own data are excluded from the requirement for access review.

Individuals may authorize their own access to development or test systems containing no Tier 2 or 3 data if they are in a position responsible for that system.
Until 12/31/2018 this Standard should be considered “best practice.” After that date, the Standard will be in full force and effect.

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.

Roles and Responsibilities

Business data governance roles (Data Trustees, Data Stewards, Data Managers, Data Custodians) defined in the University of North Carolina Policy and Standard on Enterprise Data Governance participate in the development and implementation of processes described in this Standard.

Managers of users with access to covered systems participate in the authorization, review, and decommissioning of their subordinates' access.

The CIO, IT Guardians (role defined in the Policy and Standard on Enterprise Data Governance), and other IT service providers support the implementation of access controls, document processes, and participate in requirements defined in this Standard.

Definitions

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Access Controls: Access controls determine who is authorized to have an account on UNC’s Information Technology systems, what they are authorized to do with their account, and how they are to proceed with accessing the systems which they have permission to use. Access controls are designed to protect both individual and University information.

Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges. Privileges are no longer "authorized" when a user leaves a role upon-which the authorization was based (for example, leaving a job or changing to a new position with different responsibilities).

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

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.
**Multi-User System:** A server or other system providing access or services for more than one concurrent user. Typically, a system that multiple people rely-upon to be reliably available for use.

**Privileged:** System or Application Administrators as well as users with elevated data-access privileges (beyond access to their own data) are considered "privileged" users. User accounts with higher privileges than a standard user of an application or operating system or those with access to Tier 2 or 3 information other than their own are considered "privileged" accounts. This includes administrators of servers or multi-user applications, privileged access to applications, or "sudo" access. A user who can set privilege levels for other users is an administrator and therefore "privileged." NOTE: for purposes of this document, common use of "local-admin" privileges on individual devices are not included.

**Role:** A group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.

**Sensitive Information:** Information classed 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.

**User:** Any UNC-Chapel Hill Constituent, or other individual, including campus visitors, with access to University information technology systems or services.

**User Manager:** A User Manager is any University administrator, faculty member, or staff member who supervises Users or who handles University business unit administrative responsibilities.

### Related Requirements

**EXTERNAL REGULATIONS AND CONSEQUENCES**

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.

**UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES**

- Acceptable Use Policy
- Information Security Policy
- Information Classification Standard
- Information Security Controls Standard
- Information Security Liaison Policy
- Enterprise Data Governance Policy
Contact Information

PRIMARY CONTACT(S)

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Questions</td>
<td>Information Technology Services</td>
<td>962-HELP</td>
<td>Help.unc.edu</td>
</tr>
<tr>
<td>Report a Violation</td>
<td>Information Technology Services</td>
<td>962-Help</td>
<td>Help.unc.edu</td>
</tr>
</tbody>
</table>

All revision dates:

- University Policy Review Committee: Atinuke Diver: Administrative Director, pending
- Incorporate feedback: Kim Stahl: Senior Policy and Process Lead, 3/16/2018
- Administrative Review: Matthew Teal: University Program Specialist, 3/15/2018
- Administrative Review: Lee Bollinger: Associate University Counsel, 3/14/2018
- Review by Key Stakeholders: Kim Stahl: Senior Policy and Process Lead, 3/12/2018

Attachments: UNC-Chapel Hill Policy Submission Form - IT Access Control.pdf