University of North Carolina Policy on Information Technology Access Control

Introduction

PURPOSE

The Access Control Policy states the University's strong interest 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. Adherence to this policy minimizes risk to the University resulting from unauthorized use of resources.

Access controls are implemented at UNC-Chapel Hill through the development and implementation of procedures and standards conforming to this policy. Physical controls for access to IT devices and technical controls for access to information provide a layered approach to securing the University's information systems.

SCOPE OF APPLICABILITY

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

Policy

POLICY STATEMENT

Access controls for UNC-Chapel Hill information systems are to be established in a manner that carefully balances restrictions preventing unauthorized access to information and services against the need to facilitate access for authorized users. Procedures supporting this Policy should take into account business needs and security requirements for each method of access to each application or system.

Access control takes place within the context of other University Policies and IT Standards (see references below). This Policy should be read as supporting rather than superseding provisions in related Policies, Standards, or Procedures.

ACCESS RIGHTS MANAGEMENT

Access Controls: IT Access control should be designed to address segregation of duties, protect the data from mishandling, and protect the system from unauthorized alterations. Mission Critical systems, and those
containing Tier 2 or Tier 3 information (sensitive information) must have appropriate security controls in place.

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

Access Methods: Given the nature of distributed systems, access control mechanisms and procedures must take into account any manner in which access may be granted to the system.

Access Review: Standards, Procedures, or processes must be established to regularly review access rights as appropriate. Review of privileged user accounts must take place regularly, be documented, and follow appropriate procedures.

Access Termination: Procedures or processes must be established to ensure termination of access rights when authorization ends. Removal of access rights must occur upon termination or change of role. (which may occur through the effective automated deprovisioning of accounts).

Authorization: Standards or Procedures must be established to require formal and documented authorization of access requests. Review of such requests must apply "need to know" principles, classification of the information contained within the affected system, and contractual or legal requirements for access to system and data. Granting user access must follow access control Procedures which take into account the full scope of data and system access being granted.

Emergency Access: Each University business unit is required to establish processes or Procedures to provide appropriate and necessary emergency access to Mission-Critical systems and applications.

Remote Access: Tier 2 or 3 information (sensitive information) that is stored or accessed remotely must maintain at least the same level of protections as information stored and accessed within the University network. This applies to remote access to University systems, and access to remote third-party systems from any location.

Physical Access

Standards must be defined to address requirements for the physical security of University information systems. Custodians of those systems shall adhere to such standards.

Physical access to Tier 2 or Tier 3 information (sensitive information) and mission critical computing resources must be controlled. Access to areas in which such resources are stored must be authorized by the technical unit or individual responsible for management of the area. Only authorized personnel may access secure areas and only when there is a legitimate business need.

For shared areas, such as data centers, containing Tier 2 or 3 information, it is the responsibility of the IT Guardian (See Enterprise Data Governance Policy) or their delegate to develop processes or Procedures for approval of access (including badge access), as well as processes or Procedures for regular review of this access.

ACCESS AUDIT AND REVIEW

Records of events concerning the use and management of user identities and authentication should be preserved according to the requirements of the UNC-Chapel Hill Records Retention Schedule or other governing requirements. Logging and retention should take business need for the information into account.

Appropriate audit processes based on the sensitivity of the data should be designed and implemented to identify questionable data-access activities, investigate breaches, respond to potential weaknesses, and assess the security program.
EXCEPTIONS

Exceptions to this Policy may be made by the Vice Chancellor for Information Technology and Chief Information Officer (CIO) or their delegate(s), authorized in writing. Exceptions may also be defined in the Standard for Information Technology Access Control or other related supporting Standards or Procedures.

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.

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.

Related Requirements

EXTERNAL REGULATIONS AND CONSEQUENCES

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.
Access Control Standard
Acceptable Use Policy
Enterprise Data Governance Policy
Enterprise Data Governance Standard
Incident Management Policy
Information Security Policy
Information Classification Standard
Information Security Controls Standard
Information Security Liaison Policy
Onyen Policy
Password Standards
Protocol for Responding to Security Breaches of Certain Identifying Information
Transmission of Protected Health Information and Sensitive Information Policy
Standard for the Transmission of Protected Health Information and Sensitive Information
UNC-Chapel Hill Records Retention Schedule

Contact Information

POLICY 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>ITS Policy Office</td>
<td>919-962-HELP</td>
<td><a href="mailto:Its_policy@unc.edu">Its_policy@unc.edu</a></td>
</tr>
<tr>
<td>Report a Violation</td>
<td>Information Technology Services</td>
<td>919-962-HELP</td>
<td>N/A</td>
</tr>
</tbody>
</table>

All revision dates:

Attachments:

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

Approval Signatures

<table>
<thead>
<tr>
<th>Step Description</th>
<th>Approver</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Policy Review Committee</td>
<td>Atinuke Diver: Administrative Director</td>
<td>pending</td>
</tr>
<tr>
<td>Incorporate feedback</td>
<td>Kim Stahl: Senior Policy and Process Lead</td>
<td>3/16/2018</td>
</tr>
<tr>
<td>Administrative Review</td>
<td>Matthew Teal: University Program Specialist</td>
<td>3/15/2018</td>
</tr>
<tr>
<td>Step Description</td>
<td>Approver</td>
<td>Date</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Administrative Review</td>
<td>Lee Bollinger: Associate University Counsel</td>
<td>3/14/2018</td>
</tr>
<tr>
<td>Administrative Review</td>
<td>Philip Garriss: Information Systems Auditor</td>
<td>3/13/2018</td>
</tr>
<tr>
<td>Review by Key Stakeholders</td>
<td>Kim Stahl: Senior Policy and Process Lead</td>
<td>3/12/2018</td>
</tr>
</tbody>
</table>