IDENTITY AND ACCESS CONTROLS
07.300.01

Authority:	Chief Information Officer (CIO)
History:	Approved by CIO July 10, 2021
Sources of Authority:	UNC System Office Policy Manual, Chapter 1400 "Information Technology"; International Organization for Standardization ISO/IEC 27002
Related Links:	07.100.00 Responsible Use of Information Technology Resources 07.200.00 Responsible Management of Information Technology Resources
Responsible Office:	Information Technology Services

I. Purpose

The University of North Carolina Wilmington manages data on behalf of its diverse population. To protect and defend this data from misuse and harm, we must balance access to this data, based on business need and risk. The purpose of this policy is to limit said access to information and information processing facilities to only those with legitimate business needs operating on behalf of the university.

II. Scope

This policy applies to all authentication services that provide access to resources including, but not limited to, the following identities students: faculty, staff, contractors, vendors, business partners, service providers, volunteers, part-time employees, interns, guests, assistants, systems, application program interface tokens, and service accounts.

III. Definitions

A. ID – The ID is considered any identification used in conjunction with the required authentication assurance to authorize access. Examples of ID and assurance information includes but is not limited to username and password, university identifier and pin, digital identity, and digital card reader, or the previous with the addition of any other authentication assurance information.

B. Authentication assurance – defines the level of assurance required to gain authorized access to a resource. As an example, many university systems require two factors of authentication (ID + something you know + something you have) to provide enough assurance to gain access to the resource. Authentication assurance can be any combination of something you know, something you have, something you are, or somewhere you are.

IV. Policy

A. User Access

1. Users are responsible / accountable for all activity performed with their personal IDs

2. Registration and De-Registration

a) Individual access will be granted and monitored using an ID unique to the identity and resource to which the access is being granted.

b) When the user's relationship with the university is terminated or the identity no longer required access, they shall be denied further access to university computing resources in accordance with internal procedure unless extended by an appropriate university official.

c) IDs will be reviewed at least annually, and any outdated or inaccurate access permissions will be removed.

d) IDs cannot be reassigned after being issued. Once an ID has been issued it may not be used again unless it is to the same identity with the same access as the original assignment. In the case in which a new hire happens to have been an employee of the university previously, the previous ID can be issued so long as their access conforms to and is not greater than needed for their role. If access cannot conform, then their previous ID will not be reinstated.

3. Authorization / Access Provisioning

a) Access to UNCW information resources must be authorized by the appropriate relevant custodial authority within the university.

(1) The level of access granted will be limited to those resources that are required to carry out the specified business needs of the university.

(a) Access privileges to UNCW information resources is based on their job duties and responsibilities. This is known as "role-based access." This access applies the "minimum necessary" principle.

(b) Being authorized to view or use a system does not imply access to all the information within that application or system, nor does it imply ownership.

(2) The access must be enabled for specified tasks and functions and limited to specific individuals and only for the time period required to accomplish approved tasks.

(a) In some cases, a user may be required to receive training before obtaining access to an application or system. Such prerequisites are determined by their supervisor or department and take into account the criticality and sensitivity of the role and access involved.

(3) Nonaffiliated access must be uniquely identifiable, and password management must conform to university policies.

b) For the computers and network systems, all access privileges are granted for exclusive and individual use of the individual to which they are assigned. Access to any other users' resources or any attempt to subvert access controls are strictly prohibited.

c) Access privileges must be enabled for specified tasks and functions by the appropriate relevant authority within the university.

d) When a user's role with the university is modified, access must be reviewed and modified to provide only the access required for the new role. Any such changes must be authorized by the appropriate relevant authority.

e) Nonaffiliated access to university IT resources must be authorized by the appropriate relevant authority within the university.

f) When dealing with critical or sensitive data there must be procedures for:

(1) Authorization and / or supervision of employees or affiliates who work with or are in locations where sensitive or critical data may be accessed.

(2) Determining that the access granted to sensitive or critical data is appropriate.

(3) Terminating access to sensitive or critical information when the employment of, or other arrangement with, the employee or affiliate ends or as required by the University.

B. Secret Authentication Information

Secret authentication information refers to any information used to provide authentication assurance to gain access to a system or data. Authentication information includes, but is not limited to, passwords, pins, and private cryptographic keys.

1. All secret authentication information, whether stored on-site, or using any third part data housing services, must be stored, when possible, using a cryptographic hash. If a cryptographic hash is not possible, secret authentication information must be encrypted and stored in a secure location separate from the system or service to which it relates.

2. Any transmission of secret authentication information must occur over an encrypted channel and never exposed in clear text. Exceptions can be made for temporary, one-time use authentication phrases by the appropriate university authority.

3. Secret authentication information must not be shared with other individuals or across multiple accounts provided to a single individual or service.

4. Attempting to or gaining access through the supply of false or misleading data or another user's secret authentication information, even if through negligence or naiveté, is not considered authorized use. This includes the use of "cracking" tools except when approved by and coordinated through the Chief Information Security Officer (e.g. for educational purposes in a lab environment)

5. All unauthorized use of secret authentication information must be promptly reported to the Technology Assistance Center or to ITSecurity@uncw.edu.

6. Passwords

a) UNCW password policy applies to all users and identities. All passwords must meet the appropriate complexity and security requirements as set by the university.

b) All deployed assets and services are required to change the default passwords and comply with this policy and the password requirements in the identity and access control standard.

c) Individual password security is the responsibility of each user.

d) Users must respect the policies of external networks and remote sites and only authenticate to and use facilities for which they have been authorized.

C. Applications

1. All applications that house sensitive data must require user credentials and have proper authentication methods associated with login. Additionally, access controls should be put in place on all sensitive data, allowing only users with approved permissions.

2. Application data and information can only be accessed by individuals granted rights for legitimate business needs, for the purpose of those needs.

3. Application data can only be changed, edited, or deleted by users who require that function to complete legitimate UNCW business processes.

4. Users must be authenticated and authorized to the application to be granted access to the application and system resources which house any level of sensitive data.

5. Application Program Interface access must be controlled following the principle of least privilege.

D. Access to Network and Network Services

1. Consistency between access rights and classification of systems and networks

a) User access rights will be granted to networks and systems based on business needs following the principal of least privilege.

b) Access should be determined by the relevant supervisory or delegated authority and should be in alignment with the user's business role.

2. Access controls are managed through each user's identity ID. Users must be required to provide proper ID and login credentials in order to access any network services.

3. Authentication requirements

a) All users are required to provide required authentication factors (e.g. something you have, something you know, something you are) to gain authorization to resources.

4. Monitoring / Review

a) Any activity occurring on university Networks is subject to review by appropriate personnel.

E. Segregation of Access Control Roles

1. Administrators in charge of granting access controls have several responsibilities in determining user rights as it relates to access to university resources:

a) User access must be in compliance with segregation of duties:

(1) All access requests, access authorization, and access administration must be handled by different individuals. The duties of each of these roles must not overlap each other.

(2) If limitations in personnel, or any other hindrance, makes being in compliance with proper segregation of duties impossible, additional security controls must be leveraged in order to compensate for the loss of segregation of duties and ensure against abuse.

b) For all accounts, a record of associated access permissions and changes to that access must be recorded and auditable per the retention schedule of the University.

F. Privileged Access Rights

1. In the case that elevated access must be granted to an individual for business needs, privileged access may be granted.

a) Privileged access should only be allocated to individuals after an evaluation of need and an official approval from the appropriate authority.

b) Only the least amount of privileged access should be granted to any user at any time to satisfy the business needs.

c) A record of users and access granted should be kept and maintained.

d) Privileged IDs will be reviewed at least annually, and any outdated or inaccurate access permissions will be removed.

e) Privileged ID passwords must adhere to the university privileged password requirements, and passwords must be changed as soon as access rights have been terminated.

f) Privileged access cannot be given to a generic UNCW account and must always be for a separate privileged account ID.

g) Service accounts must follow the service account password requirements and cannot be used as employee accounts. Care must be taken to reduce the service account access to the least privilege required to perform its task.