Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	June 2018
Policy 5.8.4	**Access Management**	Responsibility:	Chief Information Security Officer

ACCESS MANAGEMENT

Policy

UT Health San Antonio shall adopt access management processes to ensure that access to Information Resources is restricted to authorized users with minimal access rights necessary to perform their role and responsibilities.

- Appropriate security measures shall be implemented to ensure the protection of all UT Health San Antonio Information Resources and Data with respect to privacy, unauthorized disclosure, unauthorized modification, denial of service and unauthorized access.

- All UT Health San Antonio schools, offices and departments that create and manage access accounts for networks, servers or applications must manage the accounts in accordance with defined processes in compliance with this policy and the requirements of the UT System Identity Management Federation Member Operating Practices (MOP).

Access Control

All non-public UT Health San Antonio Information Resources must be accessed through an access control system that allows users to be individually identified and authenticated. An access management process must incorporate procedures for:

a. assigning a unique identifier for each applicant, student, employee, insured dependent, research subject patient, alumnus, donor, contractor, and other individuals, as applicable , at the earliest possible point of contact between the individual and the institution;

b. assigning a Custodian for each Information Resource or Data element responsible for:

   i. defining security profiles for group and role membership; and

   ii. account provisioning, monitoring and review;

c. enforcing password strength (e.g., complexity) that minimally conforms to the UT Health San Antonio password standards;

d. where possible, automatic log-off or password protected screen locking should be used to prevent unauthorized persons from accessing an unattended system that is logged in with an authorized account;

e. creating uniquely identifiable accounts for all users. This includes accounts created for use by third-parties and contractors;

f. disabling all generic and default accounts;

g. reviewing, removing and/or disabling accounts at least quarterly, or more often if warranted by risk, to reflect current user needs or changes of user role or employment status;

h. immediately disabling or de-activating an account when its password is assessed as potentially compromised or suspicious activity is associated with the use of the account;

i. expiring passwords or disabling accounts based on risk (e.g., termination with cause); and

j. managing access from wired and wireless devices, and from remote locations.

Passwords

Policies, Standards and Procedures defining passwords to access Information Resources shall be adopted with processes for:

a. ensuring user identity when issuing or resetting a password;

b. establishing and enforcing password strength;

c. changing passwords;

d. managing security tokens when applicable;

e. securing unattended computing devices from unauthorized access by implementing mechanisms to prevent password

guessing (e.g., lockout after multiple login attempts) and to block access to idle sessions (e.g., a password protected locking screen saver, session time-outs); and

f. ensuring that passwords are only accessed by or visible to the authenticating user, device or system.

Unless otherwise allowed by Policy, users must not share passwords or similar information, or devices used for identification and authorization purposes.

Shared Accounts

In some cases, an application or business need will require that an account be accessible for use by multiple users. In these cases, a Shared Account can be created. Shared Accounts must be approved by the Chief Information Security Officer (CISO) with a single user designated as the Primary Account Holder.

The Primary Account Holder is responsible for maintenance of the account including:

a. granting and revoking other users access to the account;

b. changing the account password when users with knowledge of the account ID and password terminate, transfer roles or otherwise no longer need access to the Information Resource and in compliance with the institution's Policies and Standards;

c. tracking user access; and

d. reporting problems and security incidents to the CISO.

If the Primary Account Holder's job function or status changes and cannot continue to be responsible for the account, it must be reestablished with a new Primary Account Holder designated. In most cases, group accounts will only be approved in situations where technological limitations of an application require group access to a single account.

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	June 2018
Policy 5.8.4	**Access Management**	Responsibility:	Chief Information Security Officer

Remote and Wireless Access

Remote and wireless access to UT Health San Antonio network infrastructure must be managed to preserve the integrity, availability and confidentiality of the institution's information. Remote and wireless access Standards and Procedures must:

a. establish and communicate to users the role and conditions under which remote or wireless access to Information Resources containing confidential data is permitted;

b. require the use of secure and encrypted connections when accessing Information Resources containing confidential data across the Internet, or across open segments of the institution's network or wireless network (e.g., use of VPN for access, SFTP for transfers, encrypted wireless); and

c. require monitoring for identifying and disabling of unauthorized (e.g., rogue) wireless access points.

Access to Network Infrastructure

Through appropriate use of administrative, physical and technical controls the Department of Infrastructure and Security Engineering is required to establish processes for approval of all network hardware connected to the UT Health San Antonio network and the methods and requirements for attachment, including any non-UT Health San Antonio owned computer systems or devices, to ensure that such access does not compromise the operations and reliability of the network or compromise the integrity or use of information contained within the network.

Data Access Control

All Information Resource Owners and Custodians must control and monitor access to data within their scope of responsibility based on data sensitivity and risk, and through use of appropriate administrative, physical and technical safeguards including the following:

a. Information Resource Owners and Custodians must limit access to records containing confidential data to those employees who need access for the performance of the employees' job responsibilities. An employee may not access confidential data if it is not necessary and relevant to the employee's job function;

b. Information Resource Owners and Custodians must monitor access to records containing confidential data by the use of appropriate measures as determined by applicable Policies, Standards, Procedures and regulatory requirements;

c. Information Resource Owners and Custodians must establish log capture and review processes based on risk and applicable Policies, Standards, Procedures and regulatory requirements.

   Such processes must define:

   i. the data elements to be captured in logs;

   ii. the time interval for custodial review of the logs; and

   iii. the appropriate retention period for logs.

d. employees may not disclose confidential data to unauthorized persons, institutions, vendors or organizations except:

   i. as required or permitted by law, and, if required, with the consent of the Information Resource Owner;

   ii. where the third-party is the agent or contractor for UT Health San Antonio and the safeguards described in institutional policy are in place to prevent unauthorized distribution; or

   iii. as approved by UT Health San Antonio Legal or Compliance Office or UT System Office of General Counsel.

Access for Third-Parties

Third-parties acting as an agent of or otherwise on behalf of UT Health San Antonio must execute a written agreement that specifies:

a. the data and systems authorized to be accessed;

b. the circumstances under and purposes for which the data may be used; and

c. that the final disposition of all University data must conform to and

comply with UT Health San Antonio policies and standards, including Section 5.8.18 "Third-Party Management of Information Resources" in the *Handbook of Operating Procedures* (HOP).

If UT Health San Antonio determines that its provision of data or access to the institution's computing environment or network infrastructure to a third-party will result in significant risk to the confidentiality, integrity or availability of such data, computing environment or network infrastructure, the agreement between UT Health San Antonio and third-party must specify terms and conditions including appropriate administrative, physical and technical safeguards for protecting the data, computing environment and network infrastructure.

Two-Factor Authentication

Two-factor authentication is required in the following situations:

a. when an employee or other individual providing services on behalf of UT Health San Antonio (such as student employee, contractor, vendor or volunteer) logs on to the institution's network using an enterprise remote access gateway such as VPN, Terminal Server, Citrix or similar services;

b. when an employee or other individual providing services on behalf of UT Health San Antonio (such as student employee, contractor, vendor or volunteer) who is working from a remote location uses an online function, such as a web page to modify employee banking, tax, or financial information; or

c. when an employee or other individual providing services on behalf of UT Health San Antonio (such as student employee, contractor, vendor or volunteer) working from a remote location uses administrator credentials (also referred to as "Privileged Access") to access a Mission Critical Information Resource or a server that contains or has access to confidential data.

Least Privilege and Segregation of Duties

Granting access to information and information systems must be based on the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	June 2018
Policy 5.8.4	**Access Management**	Responsibility:	Chief Information Security Officer

UT Health San Antonio shall adopt adequate controls to ensure separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

References

- U.T. System Policy 165 Standard 4
- U.T. System Policy 165 Standard 15