THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: AC-001.06-Third-Party Access to Account and Data	
Version 4	**Effective Date: 04/18/2016**

Responsible Office: Office of Cybersecurity	Last Review: 07/24/2023 Next Review: 07/24/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The University of Tennessee Health Science Center (UTHSC) offers electronic services to its computer users to perform work for the University in support of its mission and functions. During the course of business, legitimate business continuity reasons will arise that require access to information held on UTHSC IT Resources by third parties. The following Practice describes the process when a third-party requests access to this information.

This practice is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

All information held on UTHSC-owned IT Resources, including individually assigned accounts, mailboxes, network space, storage devices, and/or backups.

Definitions

Authorized University Officials: include Office of the Chancellor, Office of the General Counsel for Litigation holds, Executive Vice Chancellor/Chief Operating Officer, or AVC for HR as designee.

Third-Party – a company or entity that provides goods and/or services to UTHSC. The agreement between UTHSC and the third party should be a direct written contract or business associate agreement.

UTHSC Information Technology (IT) Resource: Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. servers and switches), software (e.g. mission critical applications and support systems), and information.

Responsibilities

Chief Information Security Officer (CISO) has overall responsibility of the Identification & Access Management (IAM) program at UTHSC and ensures that the program is developed, documented, and disseminated to appropriate UTHSC entities in accordance with University policies.

IAM Analyst is responsible for building the IAM program and consulting with system owners to ensure effective procedures are implemented.

Data Owner, or designee, will be responsible for approving requests for additions, changes, and deletions of access rights and privileges to data or information for individual users. The Data Owner will forward the approved requests to the system custodian for implementation.

System Custodian is responsible for implementing the approved requests using security controls.

Practice

1. **Need** - During the course of business, legitimate reasons will arise that require third-party access to information held on UTHSC IT Resources including, but not limited to workstations, email accounts, documents, servers, and/or peripherals. Should an individual user be unavailable or unable to provide permission to access these resources, or if circumstances supersede the right to privacy, University access without the individual's permission can be provided with the documented approval of a data and/or system owner.
2. **Approval** - All requests to access an individually assigned account by individuals who are not the account owner are made to the CISO or their delegate, who will obtain documented approval from the data or system owner, coordinate the request, and facilitate specific and appropriate access as necessary. Access to data and accounts is limited to the scope of the request.
    a. When legal needs require monitoring, preservation, and/or access to electronic information, the office of the General Council will request and guide the desired action.
    b. When business continuity requires access to electronic information, whether stored in an assigned mailbox, network space, on a hard drive, and/or backups, and
        i. The employee is available to receive and respond to email and no urgent business needs require continuity of communication, the employee will facilitate access as needed.

ii. The employee is unavailable to receive and respond to email and urgent business needs require continuity of communication, the employee's supervisor requests access by seeking approval from an Authorized University Official.
Examples of an employee's inability to provide consent include, but are not limited to the following:

- Administrative leave
- Unexpected leave that leads to prolonged absence
- Sudden termination
- Resignation
- Incapacitation

c. When requests for access to electronic information, whether stored in an assigned mailbox, network space, on a hard drive, and/or backups, or other locations accessible by the UTHSC account (NetID and password) of a deceased individual, documented approval from the Office of the General Counsel and the appropriate representative from the Office of the Chancellor must be obtained.

3. **Access** – When the access required is by a party outside of the UTHSC organization, i.e., contractor or vendor, access is granted via an approved remote software application. Access is supervised, and the event is recorded by the data owners or system owners.
4. **Additional Safeguards** - When access is afforded to data or information with a level 3 classification rating per GP-002-Data & System Classification, separate documented approval must be obtained from the data owner(s) before this data can be disclosed.
5. **Documentation** - The CISO or their delegate works with data owners regarding monitoring, access, disclosure, and/or the preservation and archival of requested data, and will document the request, disclosure details, the name and title of the requestor, and the reason for the request *.

No confidential information is ever to be stored in the ITS Ticketing System. Requests must be modified to ensure confidentiality.

References

1. UTSA IT Policy IT0110 - Acceptable Use of Information Technology Resources
2. AC-001-Access Control
3. GP-002-Data & System Classification
4. GP-003-Expectation of Privacy