THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: AC-001.08-Data Center Access	
Version 1	**Effective Date: 09/27/2023**

Responsible Office: Office of Cybersecurity	Last Review: 09/27/2023 Next Review: 09/27/2025
Contact: Ammar Ammar	Phone: 901.448.2163 Email: aammar@uthsc.edu

Purpose

To ensure the security, integrity, and reliability of UTHSC's data center. It establishes guidelines for accessing the data center, emphasizing restricted access to authorized ITS personnel only and mandatory sign-in requirements for all non-ITS personnel.

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

This standard applies to all members of the UTHSC community who require access to the UTHSC ITS Data Center.

Definitions

Data Center - a facility used to house computer systems, servers, and associated components, such as telecommunications and storage systems. It generally includes backup power supplies, redundant data communications connections, environmental controls, and security measures.
UTHSC ITS Personnel - Employees of UTHSC who are under the direct supervision of the ITS department.
Non-ITS Personnel - Any individual who is not part of the ITS department, regardless of their role or position at the University.
Sign-in Sheet - A documented record maintained at the entrance of the data center, capturing essential details of individuals accessing the facility, including date, time, purpose, and duration of the visit.

Responsibilities

ITS Department is responsible for maintaining the security and operational integrity of the data center, granting access permissions, and managing the list of

authorized personnel under the direction of the Chief Information Security Officer (CISO)/Chief Technology Officer (CTO).

Non-ITS Personnel is responsible for adhering to the rules laid out in this practice. They must sign in and out properly, refrain from unauthorized access, and respect all data center protocols.

Practice

1. Only authorized ITS personnel are granted unrestricted access to the data center.
2. Non-ITS personnel are prohibited from accessing the data center without a valid business reason and prior approval from the ITS department.
3. All non-ITS personnel who are granted access to the data center must sign in using the designated sign-in sheet located at the data center entrance.
4. The ITS department will maintain an updated list of personnel with unrestricted access to the data center.
5. Non-ITS personnel who require access to the data center must submit a request via email to the ITS Director of Systems or their delegate detailing the purpose and duration of their visit. The Director of Systems or above must approve the request before access is granted.
6. Upon arriving at the data center, non-ITS personnel must:
    a. Present identification to the ITS personnel on duty.
    b. Sign the sign-in sheet with their name, date, time of entry, purpose of visit, and expected duration of stay.
    c. Before exiting the data center, non-ITS personnel must sign out on the same sheet, noting the time of exit.

References

1. AC-001-Access Control