

| UT Health Science Center:<br>IT0311-HSC-A.-03 Data Center Access |                            |
|--|----------------------------|
| Version 2  | Effective Date: 09/27/2023 |

|   |  |
|---|--|
| Responsible Office: Office of Cybersecurity | Last Review: 03/01/2025<br>Next Review: 03/01/2027 |
| Contact: Ammar Ammar                        | Phone: 901.448.2163<br>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

| UT Health Science Center:<br>IT0311-HSC-A.-03 Data Center Access |                            |
|--|----------------------------|
| Version 2  | Effective Date: 09/27/2023 |

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. The “Data Center” is a restricted area and requires a much greater level of control than normal non-public ITS spaces. Only those individuals who are expressly authorized to do so may enter this area.
2. Only authorized ITS personnel are granted unrestricted access to the data center. This level of access is granted to ITS staff whose job responsibilities require such access. Individuals with unrestricted access may permit properly authorized individuals to have escorted access into the data center. When granting escorted access, the person with unrestricted access must escort the individual and ensure all access protocols are followed.
3. Non-ITS personnel are prohibited from accessing the data center without a valid business reason and prior approval from the ITS department.
4. All non-ITS personnel granted access to the data center must sign in using the designated sign-in sheet at the data center entrance.
5. The ITS department will maintain an updated list of personnel with unrestricted access to the data center.
6. 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 granting access.
7. 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.
8. All doors to the Data Center must remain locked at all times and may only be temporarily opened for periods not to exceed that minimally necessary to:
  - a. Allow officially approved and logged entrance and exit of authorized individuals

| UT Health Science Center:<br>IT0311-HSC-A.-03 Data Center Access |                            |
|--|----------------------------|
| Version 2  | Effective Date: 09/27/2023 |

- b. Permit the transfer of supplies/equipment as directly supervised by a person with unrestricted access to the area
  - c. Prop open a door to the Data Center ONLY if it is necessary to increase airflow into the Data Center in the case of an air conditioning failure. In this case, staff personnel with unrestricted access must be present and limit access to the Data Center.
9. The only exception allowed to the Data Center Access Practice is temporary suspension of these rules if it becomes necessary to provide emergency access to medical, fire and/or police officials, etc.

### Policy History

| Version # | Effective Date                     |
|-----------|------------------------------------|
| 1         | 09/27/23                           |
| 2         | 03/01/2025 - new naming convention |

### References

1. [IT0311-Information Technology Data Access, Management, and Recovery](#)
2. AC-001-Access Control