

UT Health Science Center: GP-001-UTHSC Information Security Program	
Version 5	Effective Date: 03/17/2016

Responsible Office: Office of Cybersecurity	Last Review: 06/29/2023 Next Review: 06/29/2023
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The University of Tennessee Health Science Center (UTHSC) creates, acquires, maintains, and distributes data, information, and information technology (IT) Resources in various forms. UTHSC has created an Information Security Program as UTHSC recognizes its obligation to effectively secure and safeguard this information in terms of confidentiality, integrity and availability while allowing individuals to appropriately access and share information when needed.

The Information Security Program is also designed to meet compliance requirements for data types regulated by federal or state law. This includes but is 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 data and information created, stored, processed, or transmitted while in the custody of UTHSC, the IT Resources that store, process, or transmit this data and information, as well as the individuals that have been granted access to this data and information, and Resources.

Responsibilities

The **UTHSC Chief Information Security Officer (CISO)** is responsible for information security at UTHSC Campus and the development, implementation, maintenance, and documentation of the UTHSC Information Security Program.

The **CISO** within the context of the UTHSC Information Security Program is responsible for the implementation of reasonable and appropriate security controls outlined in [NIST 800-53 “Security and Privacy Controls for Information Systems and Organizations”](#) and accepting information security risk.

The **CISO** is responsible for the review of all components of the UTHSC Information Security Program minimally every three years, and as necessary because of legal, environmental, or operational changes.

UT Health Science Center: GP-001-UTHSC Information Security Program	
Version 5	Effective Date: 03/17/2016

The CISO serves as Position of Authority required by [UTSA Policy IT0110 Acceptable Use of Information Technology Resources](#).

The UTHSC College, School, and Institute deans, directors and department chairs are responsible for ensuring compliance with the UTHSC Information Security Program and associated Policies, Standards, and Practices within their areas of responsibility.

All members of the UTHSC Community shall adhere to the appropriate roles and responsibilities as defined in [GP-001.01-Information Security Roles and Responsibilities](#).

Standard

1. UTHSC develops a UTHSC Information Security Program which puts in place reasonable and appropriate safeguards to secure and safeguard data and information the UTHSC creates, acquires, maintains, and distributes in various forms while allowing individuals to appropriately access and share information, as governed by applicable law.
2. Appropriate safeguards are determined by classification level and asset type. Reference 1 is a link to these safeguards.
3. Security controls and safeguards have been cross-mapped to applicable compliance requirements and are maintained by ITS.
4. UTHSC Information Security Program standards and practices are subordinate to the University of Tennessee policies that address the security of information.
5. A library of UTHSC security standards and practices has been published. Reference 2 is a link to an index of those standards and practices.
6. All members of the UTHSC Community are responsible and individually accountable for their actions related to security.
7. Violations of this policy may result in disciplinary action up to and including termination or expulsion per [GP-001.04-Information Security Violations](#).

References

1. [Information Security Requirements, Controls, and Safeguards \(https://uthsc.edu/its/cybersecurity/requirements.php\)](https://uthsc.edu/its/cybersecurity/requirements.php)
2. [UTHSC Security Standards and Practices](#)

UT Health Science Center: GP-001-UTHSC Information Security Program	
Version 5	Effective Date: 03/17/2016

(<https://uthsc.edu/its/cybersecurity/standards.php>)

3. [NIST 800-53 “Security and Privacy Controls for Information Systems and Organizations”](#)
4. [UTSA Policy IT0110 Acceptable Use of Information Technology Resources](#)
5. [UTSA Policy IT0121 Information Security Program Creation, Implementation, and Maintenance](#)
6. [GP-001.01-Information Security Roles and Responsibilities](#)
7. [GP-001.04-Information Security Violations](#)