THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: GP-001-UTHSC Information Security Program	
Version 2	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 03/18/2020 Next Review: 03/18/2022
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.

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 "Recommended Security Controls for Federal 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 as a result of legal, environmental or operational changes.

The **CISO** serves as Position of Authority required by UT IT Policy IT0110 Acceptable Use of Information Technology Resources.

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. *UTHSC Information Security Program* standards and practices are subordinate to the University of Tennessee policies that address the security of information.
3. All members of the UTHSC Community are responsible and individually accountable for their actions related to security.
4. 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. UTSA Policy IT0110 Acceptable Use of Information Technology Resources
2. UTSA Policy IT0121 Information Security Program Creation, Implementation, and Maintenance Policy
3. Standard-ITS-GP-004-Definitions
4. GP-001.01-Information Security Roles and Responsibilities
5. GP-001.04-Information Security Violations
6. UTHSC Information Security Program
7. NIST 800-53 “Recommended Security Controls for Federal Information Systems and Organizations”