THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: GP-001.01-Information Security Roles and Responsibilities	
Version 3	**Effective Date: 09/30/2017**

Responsible Office: Office of Cybersecurity	Last Review: 08/17/2022 Next Review: 08/17/2024
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The purpose of this Practice is to define the Roles and Responsibilities for all members of the UTHSC Community essential to the implementation of the UTHSC Information Security Program. This standard is also designed to meet compliance requirements for data 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 members of the UTHSC Community are subject to the UTHSC Information Security Program.

Definitions

UTHSC Information Security Program – a program to effectively secure and safeguard UTHSC's information in terms of confidentiality, integrity and availability while allowing individuals to appropriately access and share information when needed.

Responsibilities

Responsibilities are defined in the Practice section.

Practice

1. In addition to the responsibilities outlined in GP-001-UTHSC Information Security Program, the UTHSC Information Security Program identifies the following Roles and Responsibilities:
   a. **UTHSC Office of Cybersecurity**: a group of UTHSC employees assigned the implementation of the UTHSC Information Security Program. Specific responsibilities include:
      i. Preserve the availability, integrity, and confidentiality of information through the recommendation of the implementation of reasonable and appropriate safeguards and controls
      ii. Develop, implement, and maintain information security standards, practices, and procedures
      iii. Guide and recommend effective information security processes and practices
      iv. Analyze information security risk. Recommend and implement administrative, technical, and operational safeguards towards mitigation/remediation
      v. Monitoring of security compliance with internal and external requirements
      vi. Provide for Information Security awareness training
      vii. Timely response to, and management of, security events and incidents
      viii. Response to reporting requirements
      ix. Effective communications
   b. **Data Owner**: a senior level individual (or his/her documented delegate) overseeing and maintaining UTHSC Data or Information. Specific responsibilities include:
      i. Appropriately classify UTHSC Data or Information per GP-002-Data & System Classification
      ii. Assign day-to-day administrative and operational responsibilities to both Data Custodians for UTHSC Data or Information and Application Owners for application(s) maintaining UTHSC Data or Information.
      iii. Approving standards, practices, and procedures related to day-to-day administrative and operational management of UTHSC Data or Information and application(s) maintaining UTHSC Data or Information.
      iv. Determining the appropriate criteria for obtaining access UTHSC Data or

Information and application(s) maintaining UTHSC Data or Information.

v. Define reasonable and appropriate security controls towards the protection of the confidentiality, integrity and availability of UTHSC Data or Information

vi. Ensure that Data Custodians implement the defined security controls

vii. Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of UTHSC Data or Information

c. **Data Custodian:** an UTHSC employee who has administrative and/or operational responsibility over UTHSC data or Information. Specific responsibilities include:

i. Implement appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of UTHSC Data or Information

ii. Provision and de-provision access to UTHSC Data or Information as authorized by the Data Owner

iii. Understand and report on how UTHSC Data or Information are stored, processed and transmitted by the University and by third-party entities

iv. Document and disseminate administrative and operational procedures to ensure consistent storage, processing and transmission of UTHSC Data or Information

v. Understand and report on security risks and how security risks impact the confidentiality, integrity and availability of UTHSC Data or Information

d. **System or Application owner**: an UTHSC employee or group of employees with the responsibility to ensure that the program or programs, which make up the system or application, accomplish the specified objective or set of user requirements established for that application. Specific responsibilities include:

i. Responsible for the specific service or application.

ii. Accountable for incidents, problems, and changes that impact the service or application

iii. Implement appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of UTHSC Data or Information supported by the application.

iv. Assign and modify users to roles in the application based on need to know and least privilege.

e. **Users:** any member of the UTHSC Community authorized to access UTHSC

IT Resources. Specific responsibilities include:

i. Adhere to UTHSC Information Security policies, standards, practices, processes, guidelines, and procedures

ii. Maintain the security, confidentiality, integrity, and availability of data and information the UTHSC creates, acquires, maintains and distributes in various forms.

iii. Report violations of UTHSC Information Security Program in accordance with GP-001.04-Information Security Violations.

References

1. GP-001-UTHSC Information Security Program
2. GP-002-Data & System Classification
3. AT-001-Training and Awareness
4. IT0110 - Acceptable Use of Information Technology Resources
5. IT0123 - Security Awareness, Training, and Education
6. GP-001.04-Information Security Violations