THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: GP-001.04-Information Security Violations	
Version 6	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 01/11/2023 Next Review: 01/11/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To define practices and a formal process for Information Technology Services and the Office of Cybersecurity in the event an information security violation. 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 individuals subject to the UTHSC Information Security Program.

Definitions

Position of Authority – having official power to make important decisions. For cybersecurity, this is the Chief Information Security Office (CISO), the Chief Information Officer (CIO), or persons they report to.

UTHSC Community – faculty, staff, residents, students, contractors, and other persons who conduct, in the performance of work at UTHSC, require access to University of Tennessee information.

Responsibilities

The Office of Cybersecurity is responsible for investigating reported violations and presenting the findings to the CISO and CIO.

The UTHSC Campus Community is responsible for reporting any security violations in a timely manner following IR-001-Security Incident Response.

UT Health Science Center: GP-001.04-Information Security Violations	
Version 6	**Effective Date: 03/17/2016**

Practice

1. Every member of the UTHSC Community has the obligation to report Information security violations. Violations can be reported to the following:
   - UTHSC Office of Cybersecurity
   - UTHSC Office of the CIO
   - UTHSC ITS Service Desk
   - Police Department
   - Office of Institutional Compliance
   - UT Compliance Hotline
2. UTHSC will not retaliate against or permit reprisals against any faculty, staff, student, resident, contractor, or volunteer who reports a suspected violation of its policies protecting the confidentiality and integrity of UTHSC data or information. Allegations not made in good faith, however, may result in disciplinary action.
3. Substantiated violations of UT Policies and/or UTHSC Information Security Program protecting the confidentiality and integrity of UTHSC data or Information as determined by the Position of Authority may result in:
   - Disciplinary actions including dismissal
   - Mandatory corrective training
   - Immediate suspension of information systems access privileges
   - For employees: Notification of the individual's supervisor
   - For students: Notification of the Vice Chancellor for Academic, Faculty, and Student Affairs
   - Invocation of disciplinary sanctions under the appropriate UT and/or UTHSC policies pertaining to faculty, staff, and students
   - Any action that may be required by applicable state or federal law, regulation or contract including, but not limited to, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Family Education Rights and Privacy Act (FERPA)
   - Fees and/or fines. When appropriate and warranted, a department or unit may be held accountable for fees, charges, fines, or expenses incurred or resulting from or related to any such violation or non-compliance where the unit or department is deemed in whole or part responsible.
4. Disciplinary actions must be documented.

5. Disciplinary actions may be modified based on contributing factors. These factors, on a case-by-case basis, may include consideration of specific circumstances including, but not limited to:
   - Violation of specially protected information such as HIV-related, psychiatric, substance abuse, and genetic data
   - Volume of individuals or data affected
   - Level of exposure for the organization
   - Magnitude of organizational expense incurred, such as breach notifications
   - Hampering the investigation, lack of truthfulness
   - Negative influence on others
   - History of performance issues and/or violations
   - Work history

References

1. GP-001-UTHSC Information Security Program
2. IR-001-Security Incident Response
3. IT0110 - Acceptable Use of Information Technology Resources
4. GP-004-Acceptable Use of IT Resources