THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: GP-001.04-Information Security Violations	
Version 5	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 03/31/2020 Next Review: 03/31/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To define practices and a formal process for Information Technology Services and IT Security in the event an information security violation.

Scope

All individuals subject to the UTHSC Information Security Program.

Practice

1. Every member of the UTHSC Community has the obligation to report Information security violations. Violations can be reported to the following:
   - UTHSC ITS Information Security Team
   - Security Hotline
   - Office of the UTHSC CIO
   - UTHSC ITS Helpdesk
   - UTHSC Privacy Officer
   - 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 with a classification rating of 3 in any area. 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 with a classification rating of 3 in any area 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 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-002-Data & System Classification
2. GP-001-UTHSC Information Security
3. AT-001-Training and Awareness

4. UTSA Policy 0110 Acceptable Use of Information Technology Resources
5. UTSA Policy IT0123 Security Training, Awareness, and Education