



Security Awareness Acknowledgement: Protecting the Confidentiality and Integrity of Digital Research Data

Certain research data should not be disclosed (shared). Digital Research Data should be classified as sensitive and non-sensitive. Sensitive Digital Research Data requires higher than normal security measures to protect it from unauthorized access, modification or deletion (ex. SSNs, PHI (Protected Health Information) or HIPAA information, credit card numbers, and research data).

Responsibilities & Accountability:

The overall goal of Information Security is to protect the confidentiality and integrity of research data without creating unjustified obstacles to the conduct of research activities.

I acknowledge:

The Lead Researcher should manage and monitor access to Sensitive Research Data under their control based on Sensitivity and risk and should secure it appropriately using the following guidelines:

1. Provide access to Sensitive Digital Research Data on a need to know basis.
2. Use UTHSC-H's issued identity credentials and Access Management Procedures to provide access to computer systems, databases, web applications, etc.
3. Use Virtual Private Network (VPN) for secure remote access to the UTHSCH computer systems when access is required from off-campus.
4. When entering into an agreement with a third-party, the agreement must require the third party to use appropriate administrative, physical, and technical safeguards to protect the confidentiality and integrity of the Sensitive Digital Research Data
5. To Protect Sensitive Research Data, I should:
 - Use anti-virus with current virus definitions and firewall software.
 - Regularly or automatically upgrade and patch Operating systems.
 - Back up data regularly, protect and secure the backup, and ensure it can be reliably restored.
 - Store data only on institutional or personal computers or other electronic devices that are secured against unauthorized access and would not compromise research efforts if lost or destroyed.
 - Protect the security of Sensitive Digital Research Data during electronic communications or transmissions:
 - Use Secure File Transfer Protocol (SFTP)
 - Use encrypted email
 - Do not use non-UT email accounts (ex: Yahoo, Hotmail)
 - If data is encrypted, ensure that Information Security assists with the secure escrow of encryption keys to ensure data can be recovered in the event that assistance is required.
 - Disposal of electronic media (e.g., hard drives, CD/DVDs, tapes, etc) containing Sensitive Digital Research Data via Department of Defense (DoD) reformat, degaussing, or physically destroy
 - Physically protect access to research labs and offices.
 - Lock workstations or use password protected screen savers when systems are left unattended.
 - Physically secure portable computers, devices and media containing Sensitive Digital Research Data if left unattended.
 - Report a suspected security incident to Information Security its@uth.tmc.edu.

I accept responsibility, acknowledge my accountability, and understand my role in the protection of all Sensitive Digital Research Data.

Printed Name: _____ Signature: _____

Department: _____ Date: _____