Don't Lose Your TTUHSC Data!

Back It Up

In case of an accident, a lockout, network shutdown, or cyberattack, data kept on approved TTUHSC IT networked storage systems is securely backed up and recoverable.

What *kind* of data should be backed up?

- **Business-critical and departmental data**
  - Information necessary for day-to-day departmental operations
  - All data subject to state and federal regulations (FERPA, HIPAA, etc.)
  - For information on how TTUHSC data is classified, see: Security Categorization of Information and Information System Impact
- **Non-business-critical, work-related documents**

What is the *best* way to keep TTUHSC data backed up?

- **Only use TTUHSC IT-approved and managed devices for creating, storing, and transporting data**
  - Don't keep TTUHSC data on personal computers or laptops
  - Don't store TTUHSC data on non-approved external drives (portable hard drives or devices)
  - Don't archive TTUHSC email to your workstation's internal hard drives
- **Get in the habit of saving and storing your work data on approved storage solutions**
  - Don't save/store data locally on your computer or laptop
  - Contact the IT Solution Center for information about approved storage solutions

More information about TTUHSC policies and guidelines for storing and backing up data can be found in *these* policies and standards:

- HSC OP 56.01 Acceptable Use
- HSC OP 56.04 Data Privacy and Security
- TTUHSC IT Policy 56.22 Email
- Data Storage Standard
- TTUHSC IT Policy 56.38 Data Backup and Recovery

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER.
SECURITY CHAMPION

TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™
Information Technology Divison