Protect Your Workplace

Cyber Security Guidance

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Do NOT give any of your usernames, passwords, or other computer/ website access codes to anyone.
- Do NOT open emails, links, or attachments from strangers.
- Do NOT install or connect any software or hardware to the UT System network without permission from OTIS.
- Make back-ups or copies of all your important work.
- Report all suspicious or unusual problems with your computer to the OTIS Help Desk.

Physical Security Guidance

- Monitor and control who is entering your workplace: current employees, former employees, commercial delivery, and service personnel.
- Check for identification and ask individuals to identify the purpose of their visit to your workplace.
- Report broken doors, windows, and locks to UT System Guards or Facilities Management as soon as possible.
- Monitor and report suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, garages, and immediate vicinity.
- Report suspicious packages to UT System Guards. DO NOT OPEN or TOUCH!
- Shred or destroy all documents that contain sensitive personal or organizational information that is no longer needed.
- Keep an inventory of your most critical equipment, hardware, and software.
- Store and lock your personal items such as wallets, purses, and identification when not in use.