Guest Information Security Awareness Training

UTHealth | The University of Texas Health Science Center at Houston

To start, click the link to view Cybersecurity Awareness Training in compliance with the Texas HB 3834. Attest to Completion of this training when you sign the Information Resources User Acknowledgement Form.

Adhere to these UTHealth policies

Mobile Devices

- If mobile devices are used to access University data, email or confidential information, the mobile device must be authorized and use a "secure profile" per the UTHealth Mobile Device Policy.
- All USBs and any other portable devices must be encrypted.
- Do not store confidential information on mobile devices.
- Confidential information should only be stored on UTHealth Highest Security Zone servers.

Personally owned laptops/personal computers

- Do not store University data or confidential information on personally owned laptops/personal computers regardless of the encryption status.
- Please be vigilant with protecting UTHealth's patient information. Learn more by viewing How to Keep PHI Private & Secure.

IT Security recommends the following basic best practices while you access UTHealth resources:

1. Do not share your password with anyone!
2. Beware of phishing e-mails. Do not click on links or reply to e-mail requesting your username and password.
3. Ensure your device has anti-virus, anti-spyware and anti-malware installed and regularly updated.
4. Never use your UTHealth Password for other online services.
5. Always lock computer screen (Ctrl +Alt+ Delete) when unattended.
6. Physically secure mobile devices to prevent theft.
7. Do not use personal email to transmit UTHealth confidential data. Use UTHealth email account.
8. Encrypt all emails containing confidential information.
9. Forward suspicious e-mail as an attachment to its@uth.tmc.edu.
10. Contact IT Security at its@uth.tmc.edu if you have any questions or concerns.

updated 09/13/2024