CYBERSECURITY SAFEGUARDS FOR WORKING REMOTELY

Employees of University of North Texas institutions are responsible for adhering to the UNT System Information Security Policy and UNT System Information Security Handbook for ensuring the confidentiality, integrity, and availability of data, information, and information resources while working remotely.

Employees must ensure that personal or university-owned technology or equipment used during flexible work arrangements and remote work arrangements adhere to the protection requirements identified in the UNT System Information Security Handbook, and do not allow an unauthorized party access to university-owned data, information, or information resources. Employees are required to adhere to UNT System and university policies regarding copyright laws, intellectual property, and other policies related to use of information resources and equipment.

Cybersecurity Safeguards for Working Remotely Guide

CONNECT SECURELY TO UNIVERSITY NETWORKS AND RESOURCES

Employees should use the Virtual Private Network (VPN) when connecting to university networks or resources from remote locations. Instructions on how to connect to the university VPN can be found in the Remote Access/VPN Guide.

Avoid using unfamiliar Wi-fi networks. If you use a home Wi-fi network, ensure that the network uses strong encryption such as WPA2 protection and enable a secure Wi-fi password to protect the network from unauthorized access or use.

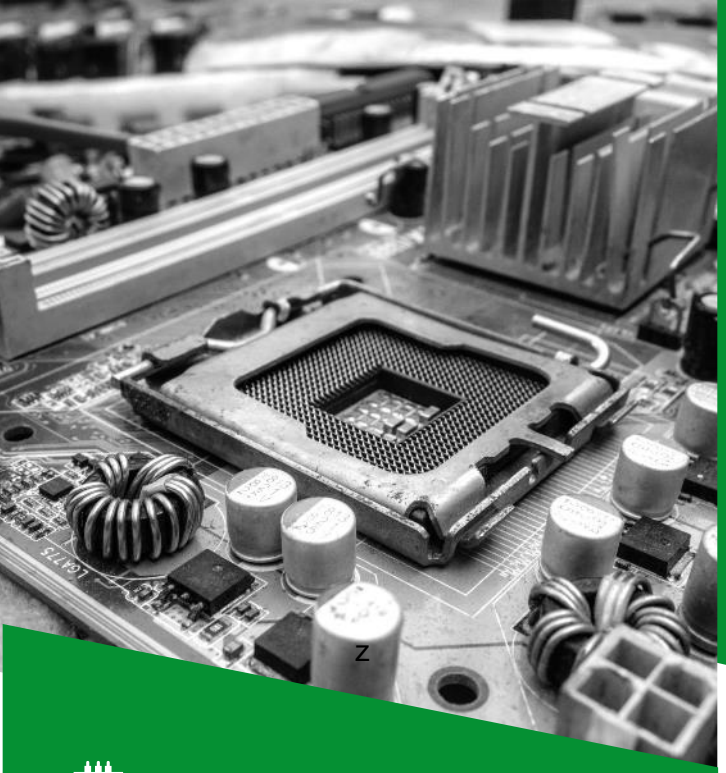
PROTECT UNVERSITY DATA

When using or handling university data, ensure that the data are backed-up and files are saved to a platform that is properly maintained. Contact local IT support staff for information on how to back-up and save files to appropriate locations.

Avoid saving your passwords in your browser in order to prevent an unauthorized individual or intruder from accessing university applications and resources.

Prevent university-owned data from being viewed by unauthorized persons. Be aware of shoulder-surfing.

Log out of devices and applications when no longer in use.



BE VIGILANT- BEWARE OF SCAMS

Avoid becoming a victim of a scam. Be vigilant about protecting your remote work environment to ensure the confidentiality, integrity and availability of university resources and data. Watch for and avoid scam emails claiming to be from sources such as the Centers for Disease Control and Prevention (CDC) or experts saying that have information about the coronavirus. There currently are no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19) — online or in stores. Beware of scams requesting donations for charities or crowdfunding sites.

Use University Approved Technology to Collaborate, Communicate and Conduct University Business

Examples of approved technology include the collection of tools available in the Microsoft Office 365 suite (Teams, Outlook, etc.). Ensure that business conversations cannot be overheard by unauthorized individuals. Keep work and personal business separate. Do not use university resources for personal use.

PROTECT PERSONALLY-OWNED EQUIPMENT

Install anti-virus software that detects, quarantines or deletes malicious code on personally owned devices. ITSS Information Security provides McAfee Antivirus software that can be downloaded online at Antivirus Download with a valid EUID and password. Ensure that physical security measures are in place to prevent damage, harm, theft or loss or personally owned devices.

Be mindful of apps that you install on your personal device. Ensure that they are developed by trusted sources and have been vetted by legitimate stores. Properly manage documents in accordance with university retention and security policies.

PROTECT UNIVERSITY-OWNED EQUIPMENT

University-owned equipment must be used in accordance with university policies and security standards.

Do not leave laptops or other university-owned devices unprotected while working remotely. Ensure that physical security measures are in place to prevent damage, harm, theft, and loss.

Do not change or disable security controls such as firewalls, encryption software, anti-virus protection, system patching and update controls, monitoring controls or change other configurations. To avoid automatically connecting to an unknown network, turn off automatic Wi-fi connections until you are ready to connect to university resources.

Do not use university equipment for personal use, store personal information on university-owned equipment, share your password or accounts, or allow family members or other unauthorized individuals to use university-owned equipment. Properly manage documents in accordance with system retention and security policies.

Getting Help and Reporting Security Incidents

If you need technical support or assistance while working remotely, submit a Help Ticket. Do not allow unauthorized individuals to access or modify university-owned devices or information.

If you suspect that you have been a victim of a scam, phishing incident or would like to report other security issues contact your local IT Helpdesk or Information Security immediately.

UNT System Service Desk	UNT UIT Helpdesk	UNT Health Science Center Helpdesk	UNT Dallas Helpdesk
https://itss.untsystem.edu/divisions/ets/sd ITHelp@untsystem.edu	http://helpdesk.unt.edu helpdesk@unt.edu	http://helpdesk.unthsc.edu helpdesk@unthsc.edu	https://oit.untdallas.edu/help-desk helpdesk@untdallas.edu

To learn more about information security, visit the Information Security website.

For more information about security requirements, please review the UNT System Information Security Policy and the UNT System Information Security Handbook.

UNIVERSITY OF NORTH TEXAS | UNT SYSTEM | UNT DALLAS UNIVERSITY OF NORTH TEXAS AT DALLAS | UNT HEALTH SCIENCE CENTER