TELEWORK SECURITY

Keep your network, data, & devices safe

PROTECT YOUR PERSONAL NETWORK

Install a firewall

- Ensure that your home network is protected from threats by purchasing a router or switch with a built-in firewall
- Change the network name (SSID) from the default name to something impersonal and distinctive to ensure your devices connect to your network only. Turn off the broadcast of your SSID to ensure it can not be found by others.
- Change the administrative login information (username and password) for your wireless router
- Do not install personal firewall software on a government furnished computer without approval
- Create a guest WiFi network for visitors and friends

PROTECT YOUR PERSONAL DEVICES

Restrict access to your computers

- Enable WiFi Protected Access 2 (WPA2) on the wireless connection and all personal devices (workstations, mobile phones, and tablets)
- Pick a strong password for WPA2; at least 8 characters long and includes a mixture of upper and lower case letters and symbols.
- Change passwords on a regular basis
- Maintain different passwords for all accounts - use a password manager
- Do not place your passwords on sticky notes attached to or near your equipment
- Do not place your passwords in your computer bag – if you do, a thief gets your equipment and your passwords
- Do not share your work computer with family and friends

Restrict access to your mobile phones

- Use a screenlock including face recognition, iris scanner, fingerprint, or a strong password
- Only install applications that are necessary
- Avoid removing your phone's default security programming ("jailbreaking") in order to customize the device
- Install Find My Phone (iOS)/Find My Device (Android) to quickly locate and remotely wipe your phone if lost
- Encrypt your files and data via your phone settings

Prevent malware

- Use a standard or restricted user account (a non-administrator account) for day-to-day activities
- Install anti-virus software and enable automatic updates
- Apply software updates and enable automatic updates
- Do not trust unsolicited calls to your phone or message pop-ups with offers of IT support
- Do not open email attachments from strangers, regardless of how enticing the subject line or attachment may be
- Report suspicious email by contacting the IT Help Desk
- Do not use free, unsecured WiFi. Use your mobile hotspot instead.
- Turn off Bluetooth when not in use

TELEWORK SECURITY

Keep your network, data, & devices safe

PROTECT YOUR PERSONAL DEVICES

Prevent device theft

- When in public, keep your devices in your sight at all times and never leave them unattended
- When parked, do not leave devices exposed in your vehicle

PROTECT YOUR PERSONAL DATA

Avoid phishing

- Do not provide personal information to or click links of unsolicited emails. If an email/text/IM asks you to go to a website you normally use, rather than clicking on the link, log in to the site as you normally would.
- Always call your bank, credit card company, or credit union directly (not with the phone number they may give you in the email) to verify

Safeguard files

- Only store and access personally identifiable information (PII) from government furnished equipment (GFE)
- Store your work on Google Drive or make regular backups of critical data using an external drive or back up to the cloud

Protect Internet of Things (IOT) Devices

- Remember, IOT devices connect to other computers, which may allow access to your device
- Keep your IOT devices up-to-date
- Change factory default passwords and enable any additional security settings
- Disable features you may not need