DEFEND THE DODIN

Do your part to protect the Department of Defense Information Network while teleworking

NETWORK UTILIZATION

DO:

- Log off of your VPN connection at the end of the work day
- Verify your local internet connection before calling your IT service desk, if you're having connectivity issues
- Use your organization-approved file sharing service/capability to share files with others
- Use your organization's approved communication and collaboration methods for official business
- Use DoD SAFE to share large files/videos (i.e., over 10 MB) with DoD and non-DoD recipients
- Limit all non mission-essential activity on government-furnished equipment (GFE) (e.g., social networking, audio and video streaming, personal shopping)
- Sign government emails
- Study and follow the Acceptable Use Policy for government systems
- Request assistance from knowledgeable co-workers for tips before calling your IT help desk
- Consider providing alternate phone numbers – other than your office phone number – on email correspondence, out of office replies, and/or voicemail for contact while teleworking
- Work offline when possible
- Vary the start times of conference calls to avoid always beginning on the hour or half hour
- Use voice and other collaboration tools (e.g., Jabber, Defense Collaboration Service [DCS]) and limit collaboration via cell phone when possible
- Disconnect from conference calls immediately when the call ends

DON'T:

- Use your GFE for non mission-essential activity (e.g., social networking, audio and video streaming, personal shopping)
- Use internet-based, unofficial audio and video on-demand and streaming services or websites
- Email large files or videos
- Leave video collaboration tools connected when not in use
- Auto forward your office phone to an off-site number unless your organization specifies it
- Hesitate to call your IT help desk if network limitations impact your mission
- Dial into phone or video conferences unless you were invited
- Leave applications running that you're not actively using (e.g., email, video, voice, etc.)

For additional information please visit: https://cyber.mil or https://public.cyber.mil

CYBERSECURITY

DO:

- Reboot your machine prior to establishing a VPN connection
- Ensure your government-furnished equipment (GFE) is patched with the latest updates
- Use GFE when possible
- Ensure your personal devices are updated with the latest operating system and security patches
- Follow your organization's GFE use and handling instructions
- Report loss or theft of GFE to your IT service desk immediately
- Close all applications you're not actively using
- Configure your home Wi-Fi according to best practices; change the password and enable encryption
- Study and know the difference between For Official Use Only (FOUO), Controlled Unclassified Information (CUI), and Unclassified information
- Familiarize yourself with adversary attack methodology (e.g., Coronavirus maps, coronavirus spear phishing attacks)
- Report suspicious activity or behavior to your chain of command
- Follow your organization's specific cybersecurity guidance
- Install "McAfee Total Protection" antivirus software (free to DoD employees) on your personal computer available on https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/antivirus-home-use

DON'T:

- Leave your computer unlocked when unattended
- Use untrusted internet or Wi-Fi connections
- Auto-forward or forward FOUO, CUI, publicly identifiable information (PII), and protected health information (PHI) from official email accounts to personal email accounts
- Open suspicious emails
- Use personal email accounts for official business
- Use personal cloud/file sharing accounts for official business
- Use any non-DoD instant messaging applications to share DoD information
- Post, store and or transmit FOUO, CUI, PII and PHI on non-GFE
- Send unencrypted PII or PHI
- Work from public locations where others can "shoulder surf"
- Click security alert/warning "pop-ups" on your GFE

V3_20220121

For additional information please visit: https://cyber.mil or https://public.cyber.mil