TELEWORK GUIDELINES FOR GRANTEES

DO

- Only use devices, such as laptops or smart phones, that are owned, managed, and protected by your organization.
- If you must use a personal device, first ensure use of personal devices is permitted by your organization's policies, then:
  - Follow organizational policy for encrypting and signing emails.
  - Require passwords to log into the device, use strong passwords, and change them frequently (including passwords for other accounts accessed from the same device).
  - If you have administrator privileges on a device, only use non-privileged profiles for daily activities and only use elevated privileges when administering the device.
  - Close all other non-work related windows and applications before and during work-related use of the personal equipment.
  - Create a separate user profile with minimal privileges for work-only use.
  - Close all work-related windows, applications, files, and documents when not in use
  - Clear browser cache when switching from work to personal use.
  - Keep the operating systems and all relevant applications up-to-date and fully patched.
  - Turn on automatic patching and run anti-virus software.
- Store work-related content on **grantee furnished Equipment (GFE)** and **grantee-approved** cloud services only. Do not forward work emails to a personal email account.
- Only use **grantee-approved** collaboration tools, including but not limited to chat and video conferencing platforms.
- Use your organization's approved methods to share files. Be mindful of the distribution of files even on organization-approved platforms. Avoid any unnecessary dissemination or copying of files.
- Log off of your remote connection at the end of the work day.
- Always require new passwords every 90 or 180 days. Set devices to immediately ask for a password to unlock them following inactivity.
- Study and follow your organization's acceptable use and telework policy on physical and information security. Ensure telework agreements are current.
- Only connect GFE to a network you are in complete control of (e.g. a secure, password-protected home network). Do not connect to a network you do not own and control (e.g. public Wi-Fi).
- Limit access to read and write files depending on role or job functions.
- Immediately terminate all access to systems and files of former employees.
- Organization accepts risk for the transmission and collection of PII by its employees

DON'T

- Use your GFE for non-work-related activity (e.g., social networking, audio and video streaming, personal shopping).
- Print work-related materials at home, unless explicitly approved by your organization.
- Auto-forward your office phone to a personal number unless explicitly approved by your organization.
- Dial into phone or video conferences unless you were invited. Upon dialing into a phone conference, always announce your name and affiliation.
- Keep files containing personally identifiable information (PII) out or unsecured.
- Keep work or participant files at home when the office re-opens.
- Share devices (e.g. with family or other household members) that are used for work.
- Forward work emails to a personal email account.
- Store work-related content on personally owned equipment (including personal mobile devices and personal cloud or file-sharing accounts).
- Leave your computer unlocked when unattended.
- Send unencrypted, sensitive content (e.g. PII).
- Connect to a network that you do not own and control (e.g. public Wi-Fi).

Adapted from the DoD Cyber Exchange Telework "Network Utilization and Cybersecurity Do's and Don't"