Workforce Cyber Hygiene

Government Furnished Equipment (GFE)

Best Practices

- Establish a VPN connection before working on your GFE.
- Use an organization-approved file-sharing service (e.g., DOD SAFE).
- Digitally sign government emails.
- Do not click untrusted links in suspicious emails.
- Follow the acceptable use policy for government systems.
- Use official voice and collaboration tools (e.g., MS Teams) and limit personal cellphone collaboration.
- Close unused applications.
- Follow your organization's GFE use and handling instructions and keep your property pass current.
- Report lost or stolen GFE to your IT service desk immediately.
- Understand the difference between Controlled Unclassified Information and unclassified information.
- Familiarize yourself with adversary attack methods (e.g., spear phishing).
- Immediately report suspicious activity on your GFE to technical support and your chain of command.
- Follow your organization's cybersecurity guidance.
- Update and reboot your GFE when prompted.
- Power down your GFE laptop before transporting it for effective disk encryption.

Practices to Avoid

- Do not leave your GFE unattended in vehicles or public spaces.
- Do not use your GFE for non-mission-essential activities (e.g., social networking, streaming, personal shopping).
- Do not use unofficial, internet-based audio and video streaming services or websites.
- Do not use personal email for official business.
- Do not use personal cloud/file-sharing accounts for official business.
- Do not use untrusted internet or Wi-Fi connections.
- Do not use public USB charging stations.
- Do not email large files or videos.
- Contact your IT help desk if network limitations impact your mission or if you observe abnormal system behavior.
- Do not leave your CAC unattended with your computer.
- Do not use non-DOD messaging apps to share DOD information.
- Do not forward CUI, PII, or PHI from official to personal email.
- Do not post, store, or transmit CUI, PII, or PHI on non-GFE devices.
- Do not send unencrypted PII or PHI.
- Mute your microphone on conference calls when not speaking.
- Do not work in public places where others can see your screen.
- Do not click on security alerts or warnings in your browser.
- Do not plug unapproved devices into your GFE.
- Do not use untrusted USB cables.

Published by DISA Risk Management Directorate - April 2025

Workforce Cyber Hygiene

Personal Equipment and Accounts

Best Practices

- Patch your devices! Ensure all personal internet-connected devices have the latest software updates.
- Use multifactor authentication on personal accounts whenever possible.
- Use biometrics whenever possible.
- Use a password manager to create strong, unique passwords.
- Set a strong Wi-Fi password and limit access to it.
- Enable strong encryption on your home Wi-Fi.
- Create a guest Wi-Fi network for IoT devices like TVs and thermostats.
- Use a separate password for your guest/shared Wi-Fi network.
- Encrypt critical personal data.
- Lock down your social media accounts and limit who can access your personal information.
- Install and update antivirus software on personal devices.
- Configure antivirus software to periodically scan your devices.
- Keep printers turned off when not in use.
- Enable a firewall to protect your home network.
- Turn off your wireless network's SSID broadcast.
- Disable remote administration of your wireless access point, firewall, and cable modem on public interfaces.

Practices to Avoid

- Do not use open or public Wi-Fi without a VPN.
- Do not allow unrestricted access to your home network.

Published by DISA Risk Management Directorate - April 2025