How to Work From Home

RULES OF ENGAGEMENT

OWA

- Use OWA in lieu of the VPN access if possible – only use VPN for access to resources other than email.
- Use a Government-issued laptop to access OWA if you have one.
- If you must use your personal computer to access OWA, ensure you have a proper Antivirus solution (e.g. Microsoft Defender—built-in to Windows 10, McAfee, etc.) and keep it up to date.
- Set up a local folder for any files you download from OWA, and purge this folder at the end of each day to ensure you don't leave any official work on your personal machine.

Mobility

- Make maximum use of your ONE-NET mobile device (iPhone) if you have one.
- Be sure to download all of the "Blackberry Work / Edit / Access" applications to get full capability, including the ability to edit documents. Contact your local support team for help in getting these apps on your phone.

VPN

- DON'T camp out on your VPN session. Allow others to take their turn. NAVNETWARCOM is implementing time restrictions on the VPN so expect to be kicked off if you are logged on too long.
- Only use VPN to access specific applications that won't work from outside ONE-NET, or to access shared network drive resources.

General

- DO protect <u>all</u> Personally Identifiable Information (PII), and Protected Health Information (PHI) data by encrypting emails and ensuring it is only sent to those with need to know.
- DO ensure that your personal machine is fully updated with ALL patches and security updates, including antivirus, prior to accessing OWA or any other DoD site.
- DON'T use any commercial email or collaboration tools (Gmail, Zoom, WebEx, etc.) to conduct official business. Use authorized tools only!
- TRY to limit "CC line" addressees (keep your audience small / focused if possible).
- DON'T send large file attachments. Try to limit file size as much as possible to minimize network impact and avoid inbox size limits. If you must share large files use DoD collaboration sites.

How to Work From Home

ADDITIONAL INFORMATION

DoD Root Certificate Download

To access DoD sites, you must download additional certificates to your computer.

https://www.public.navy.mil/nrh/Pages/MyNRH_IT_Support.aspx

CAC for a Mac

If you are installing a CAC reader on your Mac and it is running OS X 10.15 or newer your machine comes with built in CAC reader software. For older OS versions refer to the link below to access a user guide supporting 3rd party software installation.

Common Troubleshooting

- **Try using a different browser. (Most DoD sites are designed for Internet Explorer.)**
- **Try using a different certificate. (DoD sites are in the midst of transition between ID, e-mail, and PIV certificates.)**
- **Ensure *.navy.mil is in your trusted sites**
  - **Open Internet options**
  - **Click Security tab**
  - **Click Trusted Sites**
  - **Click Sites**
  - **Enter *.navy.mil and Click Add, Close, OK**

Home Use

Some workplace software is available for installation on your home computer for free or reduced prices through DoD Home Use Programs:

Microsoft Office, Visio, and/or Project: https://www.homeport.navy.mil/management/microsoft-hup/

McAfee or Symantec Anti-Virus: https://infosec.navy.mil/

Collaboration Sites

SECNAV SharePoint: https://portal.secnav.navy.mil/

FFC SharePoint: https://usff.navy.deps.mil/

CPF SharePoint: https://cpf.navy.deps.mil/

DoD SAFE: https://safe.apps.mil/

Inteldocs: https://inteldocs.intelink.gov/

DCS: https://conference.apps.mil/ (use e-mail certificate)

MilSuite: https://www.milsuite.mil/

Other Useful Websites

MNP: https://my.navy.mil/

NSIPS: https://www.nsips.navy.mil/my.policy

BOL: https://www.bol.navy.mil

FLTMPS: https://ntmpsweb.ncdc.navy.mil/Fltmps/

MilConnect: https://milconnect.dmdc.osd.mil

MyPay: https://mypay.dfas.mil/mypay.aspx

SLDCADA: https://www.sldcada.navy.mil

TWMS: https://twms.navy.mil/selfservice/

E-Learning: https://learning.nel.navy.mil/ELIAASv2p/

ESAMS: https://esams.cnic.navy.mil/

GTCC: http://www.citimanager.com/login

Defend the DODIN

THE FOLLOWING SLIDES PROVIDE RULES OF THE ROAD WHILE TELEWORKING.

DO YOUR PART TO KEEP THE NETWORK SAFE!

While teleworking you should:

- 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

While teleworking you should NOT:

- 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.)
- 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