Security Polices for Working from Home during COVID-19

Follow the below policies and procedures to ensure you keep information safe and secure while working from home.

Workspace

Only use your work computer for work and make sure you are on a Virtual Private Network (VPN). Try to dedicate a space where you can work undisturbed, to ensure others cannot hear your work conversations. If you can, close the door if others are home with you. Place your laptop in a way where others are unable to view information on the monitor.

If you have any voice-activated smart devices or digital assistants such as an Alexa, Google Home, etc., ensure the equipment is far enough away from your workspace or turned off so it is not activated by an unintentional voice prompt. Be extra alert for phishing related emails related to COVID-19 and report any suspicious activity.

Laptop and Tablets

When leaving your laptop or tablet unattended, remove the Smart Card or Yubikey and take it with you. Lock your computer and remove your Smart Card or Yubikey when you are done working. Laptops and tablets must not be left unsecured outside the workspace (e.g. at home, at a hotel, while traveling, unattended in a vehicle, etc.).

Ensure your laptop is secure if you are not at home, such as locking your doors or placing it in a locked drawer or file cabinet.

Documents

While working, documents that contain Protected or Confidential Health Information should be turned over, placed in a folder, drawer, or file cabinet if not being used. When not in use, or when done working for the day, secure those documents in a locked drawer or secure file cabinet so others cannot access it. Lastly, be sure to dispose of materials correctly, such as shredding.

Remain Vigilant and Take the Following Precautions

Scammers and phishers are taking advantage of COVID-19 concerns by running phishing campaigns. These scams include downloading important information about the virus, getting access to brand recognized sites for gathering of personal information, and fraudulent donation campaigns. To stay vigilant:

- Check the sender's email address. If the highlighted email address contains characters that aren't in the company's main website, it could be a fake email address.
- Avoid clicking on links in unsolicited emails and be wary of email attachments.
- Do not reveal personal or financial information in an email and do not respond to email solicitations for this information.

Resources

- For more information, please visit COVID-19 Resources Page
- For more Policy information:
    - Integrated employees see our Security Policy and Standards on the Hub within eGRC.

- Non-Integrated employees, see our Security Policy and Standards on the SAFE With Me Portal