CYBER SECURITY TIPS FOR WORKING REMOTELY

BASIC CYBER-HYGIENE

- Make sure that your devices are up to date with security patches.
- Use anti-virus software on all devices and keep it updated.
- Ensure that your WiFi network is encrypted with WPA2 as a minimum, and DO NOT USE public WiFi.
- Use strong, unique passphrases on each device and account.
- Utilize multi-factor authentication (MFA) for online accounts.
- Don’t click on links in unsolicited email.
- Do not give out your personal information in response to an unsolicited email, text message, or telephone call.

TELECOMMUTING TIPS

- Only connect to the work network from home through a Virtual Private Network (VPN) so that the communication is encrypted end to end.
- Research any telework application that you intend to use and ensure that it has robust security features and requires secure credentials to login and restrict access.
- Be cautious about remote desktop sharing on telework applications.
- Utilize Mobile Device Management (MDM) software on mobile devices to ensure that they can be wiped if lost or stolen.
- Encrypt removable media so that if it is lost or stolen, sensitive data is not exposed (if you work in multiple environments Mac, PC, Linux, ensure that the encryption product works across environments).