

REMOTE WORKER SECURITY GUIDELINES

IT CHECKLIST

- Enable Local encryption
- Local admin accounts are known with strong passwords
- Limit external sharing of Cloud applications (OneDrive, etc)
- Enable MDM for remote wipe capabilities
- Review and enable remote endpoint security tools that can be centrally reviewed and monitored (Cylance, Cisco Scansafe, etc)
- Provide ability to securely exchange files and information externally and internally (i.e. sharefile.com, office-365 encryption option enabled, on-premises solution, etc)
- Enable Multifactor Authentication for remote connectivity that expires after 4-8 hours of use
- Review Incident Response procedure with all relevant parties

EMPLOYEE CHECKLIST

- Secure workspace
 - Ability to lock laptop and any business relevant information when not in use
 - Safely perform conversations without visitors eavesdropping or shoulder surfing
- Wireless Security
 - Change default Wifi Router passwords
 - Enable WPA-2 or higher encryption; Strong WEP password at minimum
 - Ensure your local router firmware is updated
- Personal Device security
 - Updated IOT Device firmware (Smart Thermostats, Surveillance cameras, etc)
 - Ensure default passwords are changed
 - Updated software on all devices within your home network (Corporate laptop, IOT devices such as cameras and Smart Thermostats, personal laptops/tablets, etc)
- Review corporate policies and procedures

AWARENESS

- Corporate vs Personal
 - Do not share your corporate laptop for use with family or friends.
 - All corporate activities must be performed on the device provided by the organization
- Limit social media use
 - Don't reveal business itineraries, corporate info, daily routines, etc