REMOTE WORKFORCE

Security Checklist

IT Checklist

- [ ] Enable Local encryption
- [ ] Local admin accounts are confirmed with strong passwords
- [ ] Limit external sharing of Cloud applications (OneDrive, SharePoint, etc)
- [ ] Enable MDM for remote wipe capabilities
- [ ] Review and enable remote endpoint security tools that can be centrally reviewed and monitored (RMM, SentinelOne, NovaSOC, etc)
- [ ] Provide ability to securely exchange files and information externally and internally (i.e. OneDrive, DLP, email encryption, 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, etc).
  - Ensure default passwords are changed.
  - Updated software on all devices within your home network (Corporate laptop, IOT devices, personal laptops/tablets, etc).
- [ ] Review corporate policies and procedures.

Security 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.