CYBERSECURITY REQUIREMENTS AND BEST PRACTICES

DESKTOP/LAPTOP REQUIREMENTS

- Operating system currently supported by provider
- Antivirus installed (one of the following or equivalent)

   Windows users:
   - Windows Defender (built into Windows 10)
   - Norton 360
   - Webroot
   - TotalAV
   - McAfee
   - Trend Micro
   - VIPRE
   - Cylance
   - BullGuard

   Mac users:
   - macOS XProtect (built into macOS 13)
   - Airo
   - MacKeeper
   - Intego
   - TotalAV

- Antivirus software up to date
- Anti-malware installed (one of the following or equivalent)

   - Windows Defender (built into Windows 10)
   - Intego
   - Malwarebytes
   - McAfee Total Protection
   - Norton 360 with LifeLock Select
   - Bitdefender Total Security or Antivirus Plus
   - ESET Endpoint Security
   - Netsparker Security Scanner
   - Check Point ZoneAlarm Anti-Ransomware
   - Syxsense Secure
   - Webroot SecureAnywhere Endpoint Protection

- Anti-malware software up to date
- Screen lock set (ideally set to 15 minutes of inactivity or less)
- All critical updates and patches for operating system are applied (ideally within seven (7) days of release)
- Disk encryption required for laptops, recommended for desktops (one of the following or equivalent)

  - Windows 10 Encryption (built into Windows 10)
  - FILEVAULT (Built into macOS)
  - DiskCryptor
  - Dekart Private Disk
  - Bitlocker (included with Windows 10 Pro and Enterprise)
  - Symantec Drive Encryption
  - Rohos Mini Drive

MOBILE DEVICE REQUIREMENTS

- Operating system currently supported by provider
- Passcode, fingerprint, or Face ID enabled
- Screen auto-lock enabled
- Encryption enabled
  - The supported versions of iOS and Android have encryption built in, but may need to be activated

PASSWORD REQUIREMENTS AND BEST PRACTICES

- Password enabled
- Password best practices
  - Should be at least eight (8) total characters
  - Should be changed every 90 days
  - Should not use past passwords sequentially
  - Should include at least one lower case letter
  - Should include at least one upper case letter

PERIMETER SECURITY REQUIREMENTS

- Physical firewall enabled/installed (between firm systems and internet or outside systems)
  - In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the internet.
  - Firewalls are typically categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.
  - Most modern routers have firewalls that can be activated and configured
  - Most modern operating systems have host-based firewalls that can be activated and configured
  - We recommend using both, especially with mobile platforms such as laptops, to provide protection for equipment away from the home network

- Wi-Fi Segmentation Best Practices
    - A separate network should be provided for guests and clients, completely separate from the network used for business
    - If operating from a home office, keep the work network separate from the one used for personal and family internet
    - Most modern Wi-Fi routers come equipped with a secondary, completely separate "guest" network only requiring simple activation
    - You should not broadcast the SSID for the business network

PUBLIC WI-FI BEST PRACTICES
- Don't put anything on public Wi-Fi that you don't want the world to have
- If you need to connect away from a trusted network, most modern smart phones can be used as a hotspot. This is the safest way.
- If you require this frequently, it is highly recommended you contact your cellular provider and acquire a dedicated mobile hotspot

≋ CAMBRIDGE

For questions or more information, contact the Partner Support CTC (partnersupportctc@cir2.com) at 866-866-5005 Option 1, then Option 4

1776 Pleasant Plain Road | Fairfield, Iowa 52556 | 800-777-6080 **Compliance**