- Authentication system
    - Multi-factor authentication using a password at least 8 characters in length, no dictionary words with a mix of capital, lowercase, numbers, and special characters, in addition to a one-time passcode for logons to a new device.
    - Passwords need to be changed every 3 months.
- External website security
    - Customers will need passwords with the same requirements as above, but without the time reset.
    - HTTPS with TLS to ensure secure and encrypted connections between the web server and customers.
    - Website will maintain an active security certificate issued by a Certificate Authority.
    - Flood guards on website to prevent DoS attacks.
- Internal website security
    - Once employee is authenticated, they have access and are automatically logged in to all resources permitted for their role.
    - Access to intranet only allowed for devices approved in Active Directory.
- Remote access solution
    - VPN access for authorized users and devices through OpenVPN
    - Set up a reverse proxy server for engineers to access their work remotely with NGINX
- Firewall and basic rules recommendations
    - Use both Host-based and network-based firewalls
    - Firewall open for whitelisted applications and services based on business needs
- Wireless security
    - WPA2 with AES/CCMP encryption
    - 802.1X requirement on all access points
    - Disable WPS on access points
    - Implement Wireless Intrusion Detection System and Prevention System
    - MAC filtering
    - Monitor mode on
    - Hidden SSID and password only given upon request
    - Password changes monthly
- VLAN configuration recommendations
    - Network separation between departments
- Laptop security configuration
    - Full Disk Encryption in case of theft
    - Allow VPN to access internal network
    - Binary whitelisting for approved programs
    - Antivirus and antimalware solutions installed and updated regularly
- Application policy recommendations
    - Software package will be identical across machines
    - Software will be updated weekly during
    - Antimalware and antivirus on all devices
- Security and privacy policy recommendations
    - Lock up mobile devices when not in use.

    - Encrypt drives of company’s mobile devices.
    - Update all devices and software with patches and security updates weekly
    - Perform regular scans and tests to ensure continued security strength.
    - Maintain logs with a SIEMS in case of breach for analysis.
    - Security training for all users to educate them on good security practices.
- Intrusion detection or prevention for systems containing customer data
    - Customer data stored on server with encrypted drives
    - Limited physical access to cardholder data
    - Restrict cardholder data on a need-to-know basis
    - Encrypted transmission across public networks
    - Implement Fail2Ban for both Network and Host Intrusion Detection and Prevention Systems
    - Automatic alerts set up for all detection systems