NETWORK CHECKLIST

PASSWORD SECURITY

- ☐ Written password policy
- ☐ Password Training for all authorized users to ensure they understand the potential risks of using passwords in an insecure way.
- ☐ Inspect Workstations for written passwords in the user or server areas
- ☐ Keep password requirements documentation in a safe place

LAN SECURITY

- ☐ Hardening of servers on the internal network, removing unnecessary services and applications
- ☐ Keeping unnecessary files off of servers
- ☐ Server permissions set appropriately for users
- ☐ No anonymous users allowed
- ☐ Unauthorized login attempt policies
- ☐ Share the functions of server administration between administrators
- ☐ Limit remote administration
- ☐ Remote Access Security policy and implementation
- ☐ Disable Remote Administration where it isn't needed
- ☐ Rename Administrator Account
- ☐ Enable auditing of Administrator login attempts
- ☐ Create extra-strong passwords for Administrator accounts
- ☐ Passwords for server administration accounts should be different than workstation user accounts for the same users
- ☐ Disable Guest Account
- ☐ Restrict Access to the Everyone Group
- ☐ Create appropriate user and group accounts
- ☐ Set appropriate group access permissions
- ☐ Configure audit logs to track unauthorized access of files/systems/folders/accounts
- ☐ Configure patch management or scheduled download and application of the operating system and security patches
- ☐ Ensure Wireless Network security is configured properly, including the use of WEP, WPA2 or other wireless security protocols

WORKSTATION LOGONS

- ☐ Screen Locks on all computers
- ☐ Require passwords on all computers, including screen lock recovery
- ☐ Consider using two-factor authentication
- ☐ Harden workstations, removing unnecessary applications and programs
- ☐ Anti-virus software installed and disable circumnavigating
- ☐ Ensure anti-virus updates are occurring regularly
- ☐ Ensure software updates are occurring regularly
- ☐ Ensure the operating system and security patches are occurring regularly
- ☐ Pop-up blockers enabled

MOBILE DEVICES

- ☐ An IT security policy or BYOD policy (Bring Your Own Device) needs to be in place for mobile devices that are used on the network
- ☐ Enforcement of the mobile device policies needs to be decided on and enforced
- ☐ Wireless access points need to be secure

NETWORK EQUIPMENT SECURITY

- ☐ Configure audit logs to monitor access
- ☐ Document configuration working configuration settings in case of failure
- ☐ Document user accounts/passwords for accessing these devices and put them in a safe place
- ☐ Make sure that firmware upgrades occur regularly

ROUTER/FIREWALL SECURITY

- ☐ Use a firewall and make sure that all public-facing services are on a separate network segment or DMZ (email, FTP, web, for example) for intrusion prevention.
- ☐ Make sure that all externally sourced IP addresses are not allowed inside the LAN, but only to the DMZ
- ☐ Configure firewall policies to deny inbound access to unused ports
- ☐ Review all firewall policies for potential security risks
- ☐ Implement network address translation (NAT) where possible
- ☐ Use stateful packet inspection on the firewall, preventing IP address spoofing and DOS attacks.
- ☐ Make sure the router and firewall software is updated regularly
- ☐ Make sure the router and firewall firmware is updated regularly
- ☐ Consider having penetration testing performed for further weakness exposure