Network Security Audit Checklist

1. General

- ✓ A written Network Security Policy that lists the rights and responsibilities of all staff, employees, and consultants
- ✓ Security Training for all users regarding the use of the Network Environment and sharing data outside the company as well as allowing anybody to access their systems
- ✓ Make sure users have been trained regarding the sharing of information by email and the Internet
- ✓ All outside vendors and contractors need to sign a security agreement while they are working in your environment
- ✓ Have contingency plans in place for if and when there is a data breach or security breach.

2. 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

3. 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
- ✓ Share the functions of server administration between administrators
- ✓ Remote administration policy
    - Disable Remote Administration where it isn’t needed
- ✓ Remote Access Security policy and implementation
- ✓ 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 wireless security protocols

4. 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

5. 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

6. 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

7. 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