Network & System Security Checklist - Basic

See the "**Network and System Security Plan for SMBs**" document for more details about each item on this checklist. All the following steps are important for information security. The groups below are meant to provide priorities for your security journey.

Part 1 – Basic Security Controls

Critical: Steps 1 – 4
Very Important: Steps 5 – 8
Important: Steps 9 – 12

Critical Steps – Do these Well and Do these Now! (1 through 4)

Risk Reduction Step #1 – Network Hardening – Boundary Defense

1.1 Business-grade router installed
1.1.1 **Higher Risk Situation (or larger networks):** Standalone business-class Firewall installed
1.1.2 **If offer Internet-available resources:** Implement DMZ
1.2 Changed default and administrative passwords on all networking equipment
1.3 Wi-Fi has WPA2 security installed (or Wi-Fi disabled if not needed)

Risk Reduction Step #2 – Workstation and Server Hardening

2.1 Running updated/supported versions of operating systems. (Legitimately purchased.)
2.2 Security patches and critical updates applied to all systems on a regular basis
2.3 All unnecessary software is removed (like Adobe Flash and old versions of Java) or updated
2.4 All unnecessary services and software removed from Servers
2.5 Running updated Web-browsers, not storing passwords, with minimal plug-ins
2.6 User accounts on computers running in standard mode (no administrative rights)
2.7 Computers running updated version of Antivirus software
2.8 **Higher Risk Situation**: All computers employee full disk encryption.
2.9 **Higher Risk Situation (or larger networks):** Network segmentation (or IDS/IPS) is employed in the data center to reduce threat of lateral movement between servers.

Risk Reduction Step #3 – Traveling & Remote Workers

3.1 Full disk encryption on all laptops or machines leaving the office
3.2 Remote users always use VPN in public locations
3.3 **Higher Risk Situation (or Phase 2)**: Two-Factor Authentication (2FA/MFA) required for remote access into network. (See Note at bottom here for "2FA/MFA")

Risk Reduction Step #4 – Mobile Device Security

4.1 Smartphone security measures have been chosen and implemented on corporate and BYOD devices
Have addressed at least the following items:
4.1.1 Operating system is still supported and regularly updated with the latest security patches
4.1.2 PIN/Password required
4.1.3 Auto-lock after a certain amount of idle time
4.1.4 Remote wipe if/when device is lost
4.1.5 Device is encrypted
4.1.6 Devices are not jailbroken/rooted
4.1.7 Key apps updated regularly

Before continuing the security journey with the steps below, consider doing a high-level risk assessment to take account of your most important information assets. (Risk Assessment outlined in Part 2 of this Plan.)

Very Important Steps – 5 through 8

Risk Reduction Step #5 – Disaster Recovery Plan (with Backups)

5.1 Important data and systems are regularly backed up in encrypted format
5.1.1 Backups are checked regularly to make sure they can be used for recovery purposes
5.1.2 Backups are regularly stored offsite
5.2 A basic disaster recovery plan has been written down and can be accessed in times of data crisis
5.2.1 The D.R. plan addresses how to recover from Ransomware

Risk Reduction Step #6 – Cloud-based Security

6.1 All data stored in the Cloud is known and controlled
6.1.1 Cloud-provider chosen based on strong security technology, practices, and policies
6.1.2 Any highly confidential data stored in cloud has first been encrypted
6.2 Two-Factor Authentication (2FA/MFA) is used for all Cloud accounts that store important or confidential data

Risk Reduction Step #7 – End-User Security Awareness Training

7.1 Users are trained on best practices for security, including handling email attachments and URLs, phishing, social engineering, etc.

Risk Reduction Step #8 – Miscellaneous System Security Items

8.1 Using an email provider that has been vetted for security, including sending only encrypted emails
8.2 Running an email spam filter or other methods to reduce phishing and malicious emails
8.3 Using an encrypted password vault program to store all administrative passwords for privileged accounts
8.4 Firmware on all equipment periodically (but regularly) updated
8.5 **Higher Risk Situation (or larger networks):** A centralized log management system (or a SIEM) is deployed to help detect and respond to security breaches and incidents.

Important Steps – 9 through 12

Risk Reduction Step #9 – Security Policies

9.1 You have created and comply with security policies, addressing the following items:
9.1.1 Password Standards
9.1.1.1 Password length and complexity specified
9.1.1.2 Passwords are not reused for multiple accounts, especially business and personal accounts
9.1.1.3 No unencrypted passwords are stored in electronic format
9.1.1.4 Two-Factor Authentication (2FA/MFA) required where appropriate (e.g. remote login, Cloud accounts)
9.1.2 Protect any sensitive data written to flash drives or in backups, by encrypting it
9.1.3 Data stored in the Cloud
9.1.4 Mobile Device usage
9.1.5 Employees traveling with computers/laptops
9.1.6 Recycling computers (and printers) securely

Risk Reduction Step #10 – Control Vendor Access and Vendor Risk

10.1 Vendor access into your local systems is controlled, and not allowed without your knowledge
10.1.1 If applicable, vendors use 2FA (MFA) for access into your systems

Risk Reduction Step #11 – Security Assessments - Internal and External

11.1 Internal comprehensive & on-going Risk Assessments done for all systems and software
11.1.1 Priorities for security projects and maturity is based on risk profile
11.2 Vulnerability scans are periodically done on all internal systems
11.3 Periodic penetration testing and vulnerability assessments are performed by security experts (most likely) from an outside company

Risk Reduction Step #12 – Incident Response Planning

12.1 There is a written plan for responding to (various types of) security incidents
12.2 The incident response plan includes:
12.2.1 Contact information for internal individuals
12.2.2 External resources that might be required
12.2.3 An action item list

Part 2 – Risk Assessment

Assess Any Special Risks and Requirements

Step 1: Identify any special adversaries
Step 2: Identify all critical data assets
Step 3: Identify where critical data is stored and transmitted
Step 4: List threat scenarios for critical data
Step 5: Calculate Risk to Prioritize Cybersecurity Efforts
- How to identify risk
- How to prioritize risk

Step 6: Implement strong security controls for sensitive data based on risk

---

Part 3 – Further Risk Reduction – Info Sec Maturity

Step 1: External vendor to perform full **Penetration Test** of your network
Step 2: If you haven't yet created a security **Incident Response Plan**, do that now!
Step 3: Build **breach detection capabilities**
Step 4: Create **Disaster Recovery** and **Business Continuity** plans
Step 5: Other important information security concepts to consider as you mature your data protection program.