27-Point Network Security Checklist

This is list of suggestions is provided at no cost by COMPANYNAME. This is a list of our top recommendations but you should make your own decisions as to which of these you implement and add others that are applicable to your business. This information is supplied as-is and may be used as part of your overall data security and cybersecurity processes.

☐ 1. Firewall

A firewall is hardware or software designed to protect your business by monitoring network traffic and connection attempts to help prevent a wide variety of Internet-based attacks.

☐ 2. Anti-spam Email Scanning

Anti-spam software scan all emails for signs that they may be an attempt to compromise user's identities and/or your business' technology.

☐ 3. Antivirus and Malware Protection

These software applications scan for viruses and malware activity on your network, using a database of the definitions for billions of known issues.

☐ 4. Intrusion Prevention Solution

An Intrusion Prevention Solution is an additional layer scanning for suspicious activity. It is capable of stopping known attacks, identifying unknown threats, removing them, and blocking other threats from the same source.

☐ 5. Critical Patches & Security Updates Procedure

A procedure for managing software patches and/or updates should be created to fix or improve the program in some way, like security vulnerabilities and other bugs, and improving the usability or performance.

☐ 6. Wireless Internet Security

A Wireless Internet Security application will prevent dangerous or unauthorized access to your wireless network. You'll have control over the devices that are able to access your network and their authorization types.

☐ 7. Virtual Private Network (VPN)

A VPN is a network that enables individuals to securely access an organization's network from an external site. A VPN provides a protected tunnel through which other network activity can pass. VPNs also allow businesses with multiple locations to be on the same network.

☐ 8. Know Your Security Measures

Too often, we see CEOs and business owners who have major network vulnerabilities and have no idea what measures (if any) they're currently taking to protect their businesses network and data.

☐ 9. Have a Budget for Security

Having a specific budget for network security - separate from your overall IT budget - will be paramount if/when you need to make cuts to a budget, but need your network to remain protected.

☐ 10. Assess Vulnerabilities from Employees, Vendors, Partners, etc.

By routinely evaluating your network's risk and implementing policies to secure it, you will be able to eliminate the vulnerabilities from internal sources.

4955 Steubenville Pike, Suite 160 | Pittsburgh, PA 15205
Phone : 412-342-3800 | **Email : sales@midnightbluetech.com**

MIDNIGHTBLUE
TECHNOLOGY SERVICES

☐ 11. Assess Vulnerabilities from the Network, Applications, etc.

Software and/or hardware that has reached its end of life puts your network at unnecessary risk. Expired licenses for software likely means that you're using an outdated or even illegitimate versions of the software.

☐ 12. Keep Updates and Patches Installed and Software Up to Date

Making sure that all devices accessing your network are up to date with bug fixes and patches. Only 8% of computers receive regular maintenance and updates; known vulnerabilities that are not patched are often targeted by hackers and malware.

☐ 13. Monitor Network Traffic

When you are monitoring network traffic, it is easier to discover unauthorized devices that are attempting to access your network when you are familiar with who is allowed to be there.

☐ 14. Don't Take Risks

It is highly recommended that you block websites and applications that may be dangerous to your network, teach your employees best practices for network safety, and make sure your network and workstations have passwords that are changed periodically.

☐ 15. Implement Safe Social Media Practices

Malicious programs and applications can disguise themselves as friendly or useful tools. By discussing expected behavior with your employees and placing some limitations on social media abilities, you'll take a few more steps toward network security.

☐ 16. Inventory of All Company-Owned Devices

Knowing what you *should* have will help prevent missing inventory from going unnoticed; alternately an inventory will make it easy to identify foreign devices on your network.

☐ 17. Workstation -> Assigned User Profiles

A business may want to have employee profiles that contain information about the technology assigned to them, which software/hardware/applications they need to perform their jobs, etc.

☐ 18. UPS and Power-Saving Mode

In the event of a power outage, an uninterruptable power source (UPS) will prevent your servers from the danger of a sudden power loss by activating a reserve battery.

☐ 19. User Permissions / Statuses

By setting permissions and statuses for your employees, you're controlling the way they use technology in your office, you don't want to give an inexperienced employee super-administrative capabilities on your network.

☐ 20. Set a Schedule of Password Updates

Scheduling and changing passwords on a regular basis is a very simple thing that should be done regardless of whether it needs to be changed or not - it is a good practice to get into.

☐ 21. Remove Inactive Users from the Network

There should be a list of tasks performed when an employee leaves. Disabling their email, change important passwords (like your Wi-Fi or VPN access), remove access to your network via personal devices (see the BOYD Policy above), and other measures as you see fit.

☐ 22. Acceptable Use Policy

Have an Acceptable Use Policy, a set of rules and guidelines created by the owner of a network, website, and application to control a users' actions to prevent risks associated with the abuse of technology. Review annually.

☐ 23. Remote Access Policy

Have a Remote Access Policy in place. This type of policy is a documented outline of acceptable methods of remotely connecting to the internal network. Review annually.

☐ 24. Bring Your Own Device (BYOD) Policy

With the popularity of using personal mobile devices (such as smart phones and tablets) to perform tasks while at work, businesses should implement a BYOD policy to control the devices access to their data and network. Review annually.

☐ 25. Encryption Policy

This type of policy is critical when it comes to compliances, to ensure data safety standards are clearly understood and met by everyone on the network. Review annually.

☐ 26. Privacy Policy

To ensure that users understand that their vital information is protected, a privacy policy details how information collected will be used, disclosed, stored and managed by the company receiving the information. Review annually.

☐ 27. Email and Communications Policy

An email and/or communications policy outlines acceptable behavior and uses of a business' email along with other business communications. They often define the acceptable and unacceptable uses for that communication, i.e.: phones, fax machines, VoIP etc.