LIGHTHOUSE
IT SOLUTIONS

The Ultimate Secure-IT Checklist

STAYING AHEAD OF THE SECURITY THREATS

Protect your company's well-being. The best defense is an aggressive offence. The best way to do this is to be active in securing your data. *Passwords, networks, backups, mobile-devices, etc. are all critical places that a company cannot afford to have compromised.* Follow each item and make sure you meet top security best practices

NETWORK SECURITY AND DEVICE PROTECTION

Advanced endpoint protection is a proactive form of defense against Malware and other threats. Any device with endpoint protection is able to protect itself from anywhere and against threats that anti-virus may not detect. Firewalls are the first line of defense against intruders and can even quarantine a device from the network.

□ **Connectivity of each company network/branch is secured by a firewall appliance.**
□ **Access Control Lists of each firewall is routinely audited for unnecessary or dangerous rules.**
□ **Intrusion Detection software or appliance is implemented for detecting attacks (some industries require).**
□ **Antivirus & Endpoint Firewall is installed on computers & servers on the network.**
□ **Company employs the use of web content filtering software.**
□ **Offsite Access is restricted only to necessary persons and access is auditable.**
□ **Campus & Branch Wireless is protected by WPA2-Enterprise.**
□ **Computers and/or servers storing PII, PHI, or other protected data are encrypted, and password protected.**
□ **Mobile Devices are encrypted, and password/PIN protected in case of loss or theft.**
□ **Wireless Guest users are isolated from production network and each other (guest isolation).**
□ **Wireless networks are scheduled for availability, if possible.**

PHYSICAL SECURITY

Physical Security is the act of securing the machines that keep businesses running. This can be done through a simple server cage lock, or a closet that also has a lock. We like to make sure that there are several fail-safe's in place so that nothing happens to the servers

□ **Critical Equipment is locked and restricted to appropriate personnel. (Like locked in a closet or a server rack.)**
□ **Critical Equipment is attached to a generator and/or uninterruptible power supply.**

stop dreaming
start doing IT.

BACKUPS AND RECOVERY

Computers provide a compact manageable way to keep all your photos, recipes, reports and more. However just as easily as you could misplace an important paper, computers are susceptible to data loss as well. From accidental deletion, malware or hardware failure, there are numerous ways in which your data could be lost.

□ **Backups are performed regularly (at least daily) of all critical servers/computers.**
□ **Backups contain system state info and are able to recover a server or new hardware to a bootable state.**
□ **Backups are stored and/or replicated to at least one off-site location or provider.**
□ **Backups containing Personally Identifiable Info (PII) or Protected Health Info (PHI) are encrypted.**
□ **Backups are tested regularly (at least quarterly) for recovery.**
□ **Disaster Recovery process is documented & accounts for: File Recovery, Server Failure & Location Catastrophe.**

USER-BASED SECURITY AND PASSWORD MANAGEMENT

With role-based permissions, members or staff (or other system users) are assigned particular roles. Through those role assignments acquire the permissions needed to perform particular system functions. These permissions allow users to perform certain operations. For example, say you only want a specific level of employee to access a system or password.

□ **All employees/users are required to use their own login to access company resources.**
□ **Employee access is limited only to resources necessary to perform their duties.**
□ **Passwords and logins are not shared with other employees/users.**
□ **Multi-factor Authentication is enabled whenever possible.**
□ **Stored passwords are not saved in plain text or reversible encryption.**
□ **Passwords are complex, consisting of mixed-case letters, numbers, and symbols.**
□ **Passwords have a length at or greater than 8 characters.**
□ **Policies, procedures, logins, and important assets are well-documented and regularly updated.**

FOR MORE INFORMATION:

This checklist and the articles associated were written in the hopes that we can spread awareness in medium-small business on security. A recent update from US-CERT alerted us to the threats managed service providers face in being attacked. We hope to combat the exploitation of MSPs through both training and an open door.

This link directs you to our Inside Secure-IT article directory:
https://why.mymsp.rocks/InsideSecureIT

This link directs you to the US-CERT article on the recent threats:
https://why.mymsp.rocks/ThreatsExploitingMSPs

Contact us:
myMSP.rocks

419.740.0825
419.862.5090

sales@lighthousesol.com
info@lighthousesol.com

Lighthouse IT Solutions
Elmore, OH 43416