Cyber Hygiene Overview

Cyber Hygiene is the best practices and other activities that system administrators, organizations, and users can undertake to improve their cybersecurity while engaging in common online activities such as web browsing, emailing, texting, and connecting to networks.

Any organization utilizing good cybersecurity practices must factor in the following 3 areas:

People

Are your People prepared for cybersecurity breaches and do they have the ability to recognize potential threats? Do they understand and utilize the processes and technology in place to prevent attacks? Do they have access to training for recognizing potential threats?

Process

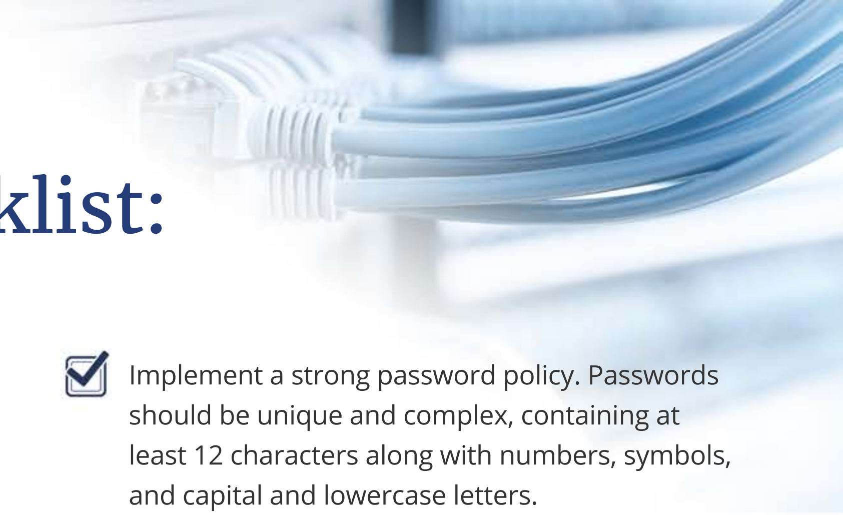
What is the process once a breach occurs? What is the process to prevent breaches in the first place? Is the plan well formulated and documented? Does the organization have a complete understanding of the IT environment overall? What is the vendor team in place to help respond to cybersecurity events?

Technology

There are hundreds of solutions in the marketplace that address cybersecurity. Some essentials include anti-virus, malware protection, firewalls, SIEM (Security Information and Event Management) tools, multi-factor authentication, identity and access management, training tools and others. Needless to say, there are several factors to consider before investing in the technology.

www.mainsailgroup.com

“Refrigerator” Cybersecurity Checklist:



- ☑ Have you assigned responsibility for cybersecurity risk management to a senior manager?
- ☑ Does this person have active and visible support from executive management at each stage of planning, deploying, and monitoring cybersecurity efforts?
- ☑ Is network and system access restricted by user and roles, such as power users, technicians, and administrators?
- ☑ Do you restrict software and firmware updates to authenticated code using methods such as signature verification?
- ☑ Do you regularly look for new ways to automatically detect when a device or network has been compromised based upon the evolving cyber world?
- ☑ Are PCs and all systems updated to the most recent software releases?
- ☑ Are all endpoints accessing the network secured including PCs, laptops, mobile devices, IoT devices?
- ☑ Implement multi-factor authentication.
- ☑ Implement a strong password policy. Passwords should be unique and complex, containing at least 12 characters along with numbers, symbols, and capital and lowercase letters.
  Passwords should be updated every 90 days.
- ☑ Disable USB ports from accessing drives.
- ☑ Is your wireless network secured and do you have a separate guest wireless network?
- ☑ Train your team on cybersecurity risks and best practices to avoid a breach.
- ☑ There are many tools available for providing automated training to end-users.
- ☑ Do you have an incident response plan? Be prepared for the unexpected with a documented policy, plan, and emergency response to a cybersecurity event.
- ☑ Have you had a risk assessment completed?
- ☑ Have you had a third-party review of your environment and plan?
- ☑ Do you have a cyber insurance policy?

About us

Main Sail, LLC (Main Sail) is an ISO 9001:2015 Certified, Veteran-Owned Small Business (VOSB), providing a wide range of business services to commercial and government clients, centered on the latest enterprise technologies, process improvement, and management disciplines.

MAIN sail

Got questions? We’re here to help.

Contact us to set up a free consultation today!