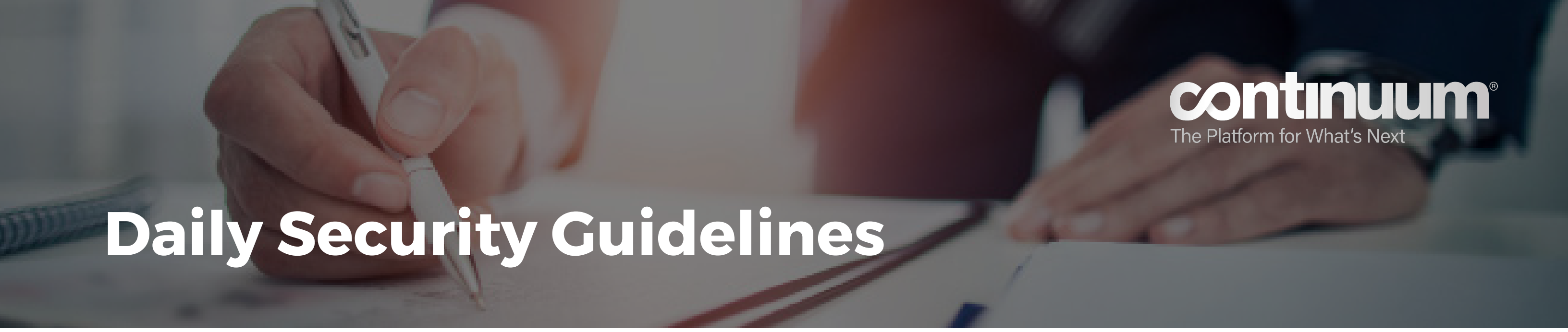

continuum®
The Platform for What's Next

Daily Security Guidelines

Employing security best practices is a constant in the life of a successful managed security services provider—and it all starts with strategy. When devising your cyber security plan of action to ensure your clients are protected from today's evolving threats, do not overlook your daily routine. Improving your security posture takes continuous education and monitoring—which means, as an MSP, you need to understand what good security looks like so you can then follow the proper guidelines, and effectively inform and protect your clients.

To get started, here is a checklist that breaks down the key areas to hone in on.

Secure your PEOPLE

The foundation of true cyber security is effective user training and education. Over half of all data security breaches are caused by human error, so it is vital that your staff, as well as your clients, are shown how to identify things like malicious email phishing attempts, and given best practices for smart and safe computing, like:

- □ Use proper password etiquette
- □ Do not leave your laptop unlocked while you're away from your desk
- □ Do not download a number of personal applications instead of using corporate-approved apps
- □ Ensure user roles and permissions are properly managed
- □ Delete credentials when employees leave the place of work
- □ Consider mobile device management for certain client environments

Threats will slip through your fingers if you fail to sharpen your security knowledge on an ongoing basis.

Secure your PROCESS

In order to prevent breaches as best you can, your business needs a solid process. Make sure you are:

- □ Effectively onboarding
- □ Providing your team continuous training and re-training on security best practices
- □ Properly evaluating the security mechanics of any new system before it's installed

In addition, it's crucial that you have an incident response plan in place— a roadmap for reducing your business' cyber security risk level and proactively minimizing damage. This plan should:

- □ Align with organizational and sector goals
- □ Consider legal/regulatory requirements and industry best practices
- □ Reflect risk management priorities

Secure your TECHNOLOGY

The final pillar that will complete your security policy is technology. Providing real security to your SMB clients requires the right collection of tools and technology. Continuum Fortify is a comprehensive solution that will ensure you can deliver complete endpoint protection, integrated in a single pane of glass. This solution allows you to:

- □ Constantly identify, prioritize and mitigate gaps in coverage
- □ Keep risk at an acceptable level
- □ Build a proactive process for each specific thing you're protecting against by setting alerts, ensuring you know where you should be focusing your attention and making updates

It is important to keep security technology best practices in mind on a daily basis. Make sure to:

- □ Keep up with your patching
- □ Review known vulnerabilities
- □ Stay up-to-date on potential issues with the tools and vendors you work with

Here's what it will look like when everything comes together and you're delivering effective security:

ADVANCED SECURITY

User Baselines | User Training | DNS Filtering | Security for Endpoints | SOC Services | Network Threat Monitoring | Log Management

- Periodic Hygiene ✓
- Attachment Scanning ✓
- Annual/Quarterly Progress Report ✓
- Perimeter Management ✓
- Recoverable Images ✓

+

- ✓ Additional Protection Vectors
- ✓ Prioritization of Protection Gaps
- ✓ Analysis Against Common Attack Patterns
- ✓ Impact Analysis of Multiple Faults
- ✓ Harm Reduction in Attack Scenario

FOUNDATIONAL SECURITY

Patching | Basic Security Services | Backup | Managed Firewall | Basic Antivirus | Periodic Vulnerability Scanning

Covering these three key bases will demonstrate your value as an MSP, the cyber security leader your clients need.