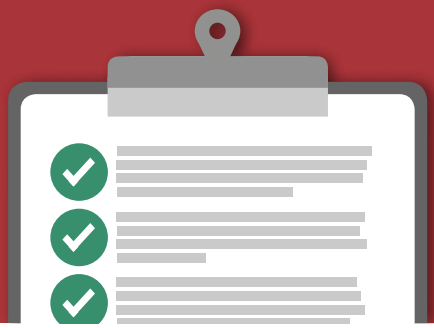
Must-Have Information Security Considerations

In order to better defend your organization against cyber threats, we recommend these measures.



Recognize how the most common successful attacks are initiated.

Foster a healthy skepticism in users so they don't just click everything they see. Never assume emails are legitimate and consider blocking certain email attachments. If something "feels wrong", go with your gut—report the incident to your security/IT team.

Enforce a rigorous password policy.

Change passwords regularly, do not share passwords across accounts (especially on public servers) or network devices, avoid dictionary terms and never use default passwords. When possible, use two-factor authentication.

Ensure that all security infrastructure is running properly.

This includes firewalls, antivirus and any other security features—all of which should receive regualar updates.

Minimize users with administrative privileges.

Always segregate "secret sauce" systems and ensure they are better protected. Disable users when they leave employment.

Log system accesses. Regularly review and look for anomolies.

Keep a detailed log history and monitor security events. Pay particular attention to authentication failures, especially ones associated with high-profile users.

Publish an Acceptable Use Policy (AUP).

Enforce an AUP among your staff. Try to address broad categories of security concerns, including software installed on end-user systems, the use of cloud providers (e.g. Gmail, Dropbox, Evernote) and personal information shared on social media sites.

Ensure backups are regularly performed.

Backups are crucial to the running of your organization and must be tested.

Implement continuous monitoring.

Implement a continuous monitoring methodology to watch for and defend against breaches.

Ensure that all patching is kept up-to-date and done so in a timely manner.

Most importantly, this includes Microsoft Windows and Office, Adobe software and all browsers.

Perform regular vulnerability assessments.

Regular vulnerability scanning can ensure that vulnerabilities are reviewed and addressed in a timely manner. Whereas a broad internal vulnerability scan should be performed at least once a year, external scanning should be performed at least once a month.

Don't forget about physical security.

This includes locking doors and encrypting portable devices.

About eSentire

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-distrupting events. Protecting more than $5 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.eSentire.com and follow @eSentire.

esentire®