



## Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: \_\_\_\_\_



## Spam Email

Secure your email. Most attacks originate in email. Choose a service designed to reduce spam and educate your staff on spam email attacks.



## Multi-Factor Authentication

Utilize multi-factor authentication. It adds an extra layer of protection to ensure your data stays protected even if your password gets stolen.



## Computer Updates

Keep products such as Microsoft, Adobe, and Java updated to ensure that your computer is secure.

### Did You Know?

**1 in 5** small businesses will suffer a cyber breach this year

**81%** of all breaches happen to small to medium sized businesses

**97%** of breaches could have been prevented with proper technology



## Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.



## Passwords

Apply security policies on your network. Examples: Enable enhanced password policies, set user screen timeouts, and limit user access.



## SIEM/Log Management

Uses big data engines to review all events and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.



## Web Gateway Security

Cloud-based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds before they reach users.



## Mobile Device Security

Cybercriminals are counting on you to neglect this part of your network. Ensuring mobile device security is important to close this gap.



## Advanced Endpoint Detection & Response

Protect your data from malware, viruses, & cyberattacks with advanced endpoint security. Use technology that protects against file-less & script-based threats.



## Security Awareness

Train your user often! Teach them about data security, email attacks, and your policies and procedures.



## Firewall Protection

Turn on Intrusion Detection and Intrusion Prevention features. Send log files to a managed SIEM.



## Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email), and especially on mobile devices.



## Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Be sure to test your backups often.