# IT Security Checklist

Associations and small to medium businesses are a prime target for malicious actors looking for member information and confidential records. Both state sponsored agents and your average hacker are looking to make money off your data and are constant threats. We want to arm you with a checklist that provides you with actionable tactics that you can put into practice today to help your organization become better prepared.

- ☐ **Conduct a security assessment** – Understand the security threats (e.g., downtime from ransomware) to the confidentiality, integrity and availability of your data. Consider the impact a breach may have on your business (lost revenue or member confidence). Use this information to shape a security strategy that meets your specific needs. Understand what points of entry exist for third party providers. Understand what protections exist in your membership system providers' operations.

- ☐ **Train your employees** – Cybersecurity threats are constantly evolving. A semi-annual training plan should be implemented for all employees. This should include examples of threats as well as instruction on security best practices (e.g., lock laptops when away from your desk). Employees are your first line of defense; helping them realize their critical role in the security of your organization will help with adoption and adherence to security policies.

- ☐ **Protect your network and any devices that connect to it** – Implement a password policy that requires strong passwords that expire every 90 days. Ensure your firewall, VPN, and antivirus technologies are up to date and protecting your endpoints from current attacks. If possible, implement multifactor authentication. Ongoing network monitoring should also be considered essential.

- ☐ **Control physical access to computers** – Use key cards or similar security measures to control access to facilities. Ensure computers are automatically locked after a period of inactivity. Encrypt hard drives.

- ☐ **Keep software up to date** – *Pre-requisite: Have visibility in to what software is installed on your devices.* It is essential to use up-to-date software products and be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.

- ☐ **Create a cybersecurity incident plan** – When it comes to cyber incidents there has been a clear shift from "if" to "when" one may occur at any given organization. When the time comes it is imperative to have a clear plan that outlines the roles and responsibilities of everyone involved. This is not only important for your team; insurance companies may not accept a claim if a plan was not followed.

- ☐ **Create straightforward cybersecurity policies** – Write and distribute a clear set of rules and instructions on cybersecurity practices for employees. This will vary from business to business but may include policies on social media use, bring your own device, authentication requirements, etc.

- ☐ **Back up your data** – Daily backups are a requirement to recover from data corruption or loss resulting from security breaches. Ensure you are using a modern data protection tool that takes incremental backups of data periodically throughout the day to reduce the risk of data loss. Test the backups periodically by doing a test restore to make sure they really work.

- ☐ **Know where your data resides** – Maintaining oversight of business data is an important piece of the security puzzle. The more places data exists, the more likely it is that unauthorized individuals will be able to access it. Avoid "shadow IT" with business-class SaaS applications that allow for corporate control of data and policies that limit where employees can put corporate data. *Bonus points: Monitor common collaboration tools that you do not support for accounts from your domain.*

Our goal is to help you is understand why IT security is a necessity and is a fundamental piece of your businesses stability and success. We also know that organization's IT security is a complex job and you need a trustworthy IT Service Provider to keep things up to date and working well. The ATS security team is available to answer any questions you may have.