ENTERPRISE
INTEGRATION

Getting Started with Cyber Security

The first step to securing your networks and developing a data security plan is to understand where you are now. Take a look through this brief checklist to assess where your organization stands now on these important issues.

- [ ] **Strong Password Policy**

  Your organization has implemented complex passwords and password-expiration policies.

- [ ] **Two-factor Authentication**

  Your organization has deployed a second method of verifying the identity of your users such as Google Authenticator.

- [ ] **Password Manager**

  Your organization uses a central program to encrypt and store complex passwords.

- [ ] **Single Sign-On**

  Your organization uses a single-sign-on methodology to let users use a single account on multiple services.

- [ ] **Control Physical Access**

  Your local servers are secured with locks and security cameras. Additionally, your data centers control access to the physical machines that house your systems.

Clean Desk Policy

Your policy requires employees to keep their desks clear of account information or other sensitive data.

Software and Firmware Patching

Your internal policies require everyone to keep servers, PCs and other endpoint devices up to date with the latest patches.

VPN and Cloud Storage for Remote Workers

Remote workers are required to connect via VPN and are prohibited from using USB and other storage devices.

Secure Off-Site Backup

All of your servers and other data is backed up securely off site.

You Work with Secure Partners

Payment processors and other integration partners have security policies that are as good as or stronger than your own.

SSL Encryption

Your company website and other computer systems use SSL encryption.

Employee Training

Your employees are fully trained on your data security policy and other best practices to avoid cyber-attacks.