USA TODAY CLASSIFIEDS BLOG

10 TIPS FOR A STRONG BUSINESS CYBER SECURITY POLICY

Almost all businesses today leverage technology to reach more customers as well as enable online sales and other operations. This means businesses will always use technology to collect, store and manage sensitive customer records and transaction information.

As such, a well-planned cyber security policy can help safeguard these records against theft or loss.

Cyber security for large and small businesses is vital to preventing scams, attacks or hacks of digital records. One breach of confidential information could place a substantial financial burden on them or their customers. There are a lot of resources out there to help develop a policy that can fight off these security risks.

Read further to learn about the components of a cyber security policy and how you can tailor that policy to fit your unique business format.

What is a Cyber Security Policy?

A cyber security policy is a written plan that outlines the methods a company will use to protect its technology and information assets. The policy advises employees on their responsibilities and obligations for protecting these assets. These policies can also outline employee and contractor levels of access.

A cyber security policy is also a preventative tool to help identify and head off threats before they do their mischief. Cyber security policies should always contain procedures for responding to security incidents as well as preventive measures to keep them from ever happening.

Cyber Security Policy: What Should I Include?

The following components should be the basic foundation of your cyber security policy:

Prepare employees on cyber security policy components

Coach your staff and other company members on your business IT security policy. Outline how you need their help to protect sensitive customer data and other digital assets. Teach them about their responsibilities and make sure they understand the role they play in safeguarding records.

Limit physical access to company computers and establish user accounts for each employee

Each individual who can access your company data should have their own user account. A single employee should be responsible for system administrative tasks. Lock and store company mobile devices or laptops when not in use.

Passwords and authentication

Staff should have their own strong password that they update every three months. Install multi-factor authentication that requires extra information beyond a password to log in.

Restrict access to data and authority to install software

No single employee or contractor should have access to all data systems. Employees only need access to the data or networks that they need to do their jobs. Staff members should also not install software programs without prior approval.

Secure an SSL (Secure Sockets Layer) Certificate to Establish Online Credentials

An SSL certificate authenticates the identity of a website and encrypts data sent on the internet. Encryption means mixing up data into an unreadable format and then returning it to a readable format with a proper decryption key. Encryption helps prevent access to personal records from unauthorized parties.

Use current or updated software on all computers and networks

Use the latest web browser versions and security software to defend against malware, viruses and other online threats. Scan your systems with antivirus software after each update.

Provide firewall security for your Internet connection

Verify that your system's firewall is on so and working so that unauthorized parties can't access data on your network. Install these firewalls on any computer equipment used by employees who work at home. Free firewall software is available online and easy to download.

Safeguard all Wi-Fi networks

Protect your company Wi-Fi network and ensure it's encrypted and hidden. You can hide your Wi-Fi network's Service Set Identifier (SSID) on your wireless access point or router. Be sure that access to your router is password protected.

Protocols for any mobile device

Make sure staff with mobile devices (i.e., phones, laptops) have password-protections on these devices. They should also install security apps to protect data while the device is on a public network. Establish protocols for reporting lost or stolen equipment.

Produce backup copies of data and other critical business information

Establish a schedule for regular backups of data on all your company's computers. Back up documents like spreadsheets, human resource files, and accounts receivable/payable records. Keep these backup copies either in the cloud or stored offsite.

Cyber Security Policy Templates Available:

Many private and public organizations share security resources that are free to use or adapt to your own organization. These templates are especially helpful for small business cyber security planning. Smaller firms can't always hire trained cyber security professionals to fight off cyber threats.

The Federal Communications Commission developed the Cyber Security Planning Guide to help a business create a cyber security plan. This guide has policy templates that companies can customize to fit their company's needs.

The SANS Institute of Philadelphia also provides resources for information security. You can find cyber security policy tools and templates on their website here.

Next Steps:

Schedule a meeting with your company's senior management today. You're going to need their support to help you get the resources you need to design your cyber security policy. Show how cyber threats can jeopardize your company's hard-earned reputation.

If you are a small business owner, remember that it's your responsibility to keep your confidential records safe. Access the templates and other resources from agencies like the Federal Communications Commission. Those agencies can help smaller, less secure businesses avoid becoming easy targets for cyber crimes.

Communicate your cyber security policies to all employees and contractors. Schedule training or briefings on the latest security software updates. Your staff should always know the vital role they play in keeping the company's digital records safe.

Track and revise your policy as appropriate. Make changes to your policy as your business mission changes or as new technology trends emerge. Develop a schedule for re-assessing your policy and whether your organization is meeting its' security goals.

Hackers, human errors and system malfunctions are all realities for every business owner who wants to do business online. Develop your cyber security policy today so that you won't become the victim of a security breach that might happen tomorrow.

You can read more about cyber security basics for businesses at the USA Today Classifieds blog.

BLOG:

Auctions
Automotive
Business
Business Spotlight
Careers
Education
Marketplace
Notices
Real Estate
Services
Sports and Recreation
Travel