BUSINESS BANKING

Cybersecurity Plan

Webster Bank

1. Password Integrity

[Enter text – Note the steps you take to keep passwords safe. For example, passwords that include special characters, last password, and your password policies.]

2. Multi-Factor Authentication (MFA)

[Enter text – Record how you use MFA in your business. Outline which processes have MFA and which don't and why.]

3. Email Security

[Enter text – Explain how you lock emails so only authenticated users can send emails from your domain.]

4. Systems Access

[Enter text – Explain how you restrict access to systems and networked equipment, software or data.]

5. Regular Backups

[Enter text – Outline your back-up process to keep data safe.]

6. Secure Wi-Fi

[Enter text – Outline how you keep wi-fi secure, including if you offer access for your customers or the public.]

7. Security Policies

[Enter text – Outline your security policies or list the security documents you have in place.]

8. User Education and Accountability

[Enter text – Explain how you ensure your employees understand your security policies.]

Cybersecurity Plan

In this plan, you'll go over essential cybersecurity and data protection activities, such as ensuring robust password strength, implementing multifactor authentication, and securing your Wi-Fi against potential threats.

Here's what you need to consider about cybersecurity.

1. Password Integrity

Write down all the steps you've taken to implement strong password policies. This includes enforcing strong, complex passwords, requiring regular password updates, and implementing screen lock passwords for all accounts and devices. Include specific information, such as whether you have password requirements, a mix of uppercase and lowercase letters, numbers, and special characters.

If you require employees to use a password manager, which is an app that stores passwords, note this as well as any other password requirements. For example, you may require employees not to use the same password for personal or other professional accounts.

2. Multifactor Authentication

Multifactor authentication (MFA), including two-factor authentication, is a means of protecting information and accounts that requires users to provide at least two different forms of verification or credentials to show they are allowed to access the system. MFA can be used to protect emails, financial information, computer systems, remote systems, and cloud services from unapproved access.

Write down the steps you've taken to implement MFA in your business, such as requiring a username and password combination as factor one and using a one-time code, smart card, or security key as factor two.

3. Email Security

Secure email systems prevent outside users from accessing sensitive information and sending emails that look as though they have come from your company. Steps taken to secure emails include having robust password policies, requiring multi-factor authentication, using encryption, and implementing security protocols. Additional steps include employee training and regular audit and monitoring.

Write the steps you take to ensure your email is kept secure and safe from outside use.

4. Systems Access

It's important to limit access to sensitive data and systems to only those people who need that access to complete their work.

Write a list of all your sensitive data and systems, as well as the roles or job titles of people who would need access to them. Include how you restrict administrative access to those crucial systems and how frequently you review user access rights to revoke any unnecessary privileges.

Where necessary, include information about any third-party vendors and contractors who may need temporary or permanent access to your data, as well as how you verify their identify and prevent any unapproved outside access. Finally, note any steps you take to monitor accounts and address suspicious activity.

Cybersecurity Plan

5. Data Backups

Performing regular backups of essential data ensures your business is protected against data loss in the case of a cyber incident. Define your protocols for data backup and recovery, including how often data is backed up, where it is stored, and how its reliability is verified. Make sure the data is encrypted during the process, to protect it in case it is compromised.

If you have policies requiring employees to back up their personal devices or their accounts, include these in the plan. Having an immutable backup is critical for organizations that need to ensure they have a copy of recoverable data that remains secure from unforeseen and undesirable accidents or incidents.

An immutable backup or storage refers to data that is fixed, unchangeable, and undeletable. Once an organization stores an immutable backup, it remains unchanged or unaltered, which is important for protecting against malware and ransomware.

6. Secure Wi-Fi

Outside users may be able to access your company network, which is why it's important to use strong encryption and change the default credentials on Wi-Fi routers. If you regularly have outsiders on your premises who need access to Wi-Fi, set up a guest Wi-Fi network to keep guest devices separate from your internal devices.

Additional steps include avoiding using your business's name or information that can identify your network, using a strong pre-shared key, and regularly updating your firmware. You can also implement intrusion detection and prevention systems to guard against suspicious activity.

7. Security Policies

Outline the steps you take to protect your systems. If you have a variety of security documents, list them along with where they can be accessed. If you have a task force, Chief Information Security Officer, committee, or compliance officer responsible for ensuring your company's cybersecurity, identify that person or their role and their responsibilities. Also note how you keep current with changes in cybersecurity trends and regulations. Include a policy prohibiting the execution of financial transactions solely based on email or messaging (SMS/Text) instructions (another form of verification, e.g., phone or in-person is required). This precautionary measure mitigates the risk of falling victim to business email compromise or (BEC) or unauthorized access and helps to safeguard against potential monetary losses and data breaches.

8. User Education and Accountability

Your employees are an important line of protection. Ensure they understand the importance of safeguarding your data and their role in maintaining your security. Make sure you have all your policies written and accessible and go over the policies with your employees so you can answer their questions. Invest in ongoing training, so your employees stay up to date with changes and best practices in cybersecurity and can watch for any suspicious activity.

If employees use personal devices for work, implement policies for those devices, such as security requirements and protocols. If employees conduct remote work, ensure you have guidelines for the remote work that maintain your security. Educate employees on common threats and safe browsing habits, as well as the importance of password protection.