Cybersecurity
Plan

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

Use this as a framework for creating detailed cybersecurity policies — consider creating an internal policy for staff and an external policy for customers.

- **The internal policy** is detailed and confidential, outlining team responsibilities, password protocols, and sensitive procedures. It is not publicly accessible.
- **The external policy** should be available on your website, and offer a general overview of how you manage and protect customer data — including responses to security incidents.

Completing your plan

1: Password integrity

Document all the steps you've taken to implement strong password policies. This should include enforcing complex passwords, requiring regular updates, and implementing screen lock passwords for all accounts and devices.

You might also consider biometric identification (face and fingerprint recognition) as well as, or instead of, passwords (biometric login options are built into many laptop and mobile devices, for example).

Be specific about your password requirements, such as the need for a mix of uppercase and lowercase letters, numbers, and special characters, not using the same password for personal and professional accounts, and whether users must employ a password manager.

This content is for general information purposes only. It is not to be relied upon as financial, tax, or investment advice or guarantees about the future, nor should it be considered a recommendation to buy or sell. You should consult your own professional advisor for specific financial, investment, and/or tax advice tailored to your needs to ensure that individual circumstances are considered properly and action is taken based on the latest available information.

coastcapital

2: Multifactor authentication

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

Document the steps you've taken to implement MFA in your business. This might include requiring a username and password combination as the first factor and using a one-time code, smart card, or security key as the second factor.

3: Email security

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

Securing emails is crucial to prevent unauthorized users from accessing sensitive information and sending fraudulent emails that appear to come from your company. Ensure that your password policies are used on email accounts.

Human error can be one of the biggest security risks for email, so awareness training about phishing scams, business email compromise (BEC), and spoofing can be a vital protection measure.

Consider integrating spam filters, malware scanning, data exfiltration (data theft) protection, and robust data retention systems. Your email service provider may offer these tools as an add-on service.

4: Restricting system access

If you have policies requiring employees to back up their personal devices or their accounts, include these in the plan.

It's important to limit access to sensitive data and systems to only personnel for whom that access is essential.

Start by listing all your sensitive data and systems, along with the roles or job titles of individuals who require access. Detail 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.

In the event of a security incident, having reliable backups is the fastest way to restore normal operations.

5: Back up your business data

As a business owner, safeguarding your data is crucial. Regular backups ensure that if your data is lost or compromised, it can be restored quickly, minimizing downtime and disruption.

Define your protocols for data backup and recovery, including the frequency of backups, storage locations, and methods for verifying reliability. Ensure that data is encrypted during the backup process to protect it in case of compromise.

Whether you handle backups internally or use an external IT service provider, you need to:

- Understand what data is being backed up
- Know the frequency of the backups
- Decide how long to retain the backups
- Know where and how offline copies of the backups are stored

6: Secure Wi-Fi

External 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' name or any 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 alongside details of where they can be accessed. If you have a task force, committee, or compliance officer responsible for ensuring your company's cybersecurity program, identify that person or their role and their responsibilities. Additionally, mention how you stay updated with changes in cybersecurity trends and regulations.

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 work remotely, ensure you have policy standards for remote work that maintain your security efforts. Educate employees on common threats and safe browsing habits, as well as the importance of password protection.

Offsite employees and remote workers present a security risk, with mobile devices like laptops, phones and desktop computers on less secure Wi-Fi networks.

This content is for general information purposes only. It is not to be relied upon as financial, tax, or investment advice or guarantees about the future, nor should it be considered a recommendation to buy or sell. You should consult your own professional advisor for specific financial, investment, and/or tax advice tailored to your needs to ensure that individual circumstances are considered properly and action is taken based on the latest available information.

Cyber Security Plan

1. Password integrity

[Enter text – Note the steps you take to keep passwords safe. For example, passwords that include special characters, last pass, 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. Restricting systems access

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

5. Back up your business data

[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.]

coastcapital