Checklist

HarborOne U VOYAGE FOR BUSINESS

Cyber Security

Cyber security is a constantly changing threat landscape that can leave organizations vulnerable. These measures can help protect your organization.

	Done	
Password Integrity	**Yes**	**No**
1. Identify where passwords are required	☐	✔
2. Write a password policy	☐	✔
3. Configure applications and systems to enforce the policy	☐	✔
Multi-Factor Authentication (MFA)		
1. Choose a MFA solution for the company	☐	✔
2. Choose applications where MFA is required and setup to enforce MFA on logins	☐	✔
3. Set-up each employee with MFA access	☐	✔
Email Security		
1. Identify all email services that send email from your address	☐	✔
2. Review email security DNS settings to identify issues and update where necessary	☐	✔
3. Set up email monitoring so you can be notified of any issues	☐	✔
Secure Wi-Fi		
1. Check that wifi networks are secured	☐	✔
2. Set up a separate wifi network for customers (if required)	☐	✔
Systems Access		
1. Identify systems (hardware and software) that need to be locked down	☐	✔
2. Set up user access levels where appropriate on systems	☐	✔
3. Set up each user with appropriate access levels on systems	☐	✔
4. Provide locked cabinets for items that must be secured (e.g., backup drives, cash)	☐	✔
5. Install anti-virus software and firewalls on systems	☐	✔
6. Install security cameras that can monitor who is accessing systems	☐	✔
Regular Backups		
1. Set up cloud based backups for critical data	☐	✔
2. Set up physical back up hardware	☐	✔
3. Decide who will store copies of physical data and where	☐	✔
Security Policies		
1. Assign a person to manage security policies	☐	✔
2. Create a security policy document that all staff can access	☐	✔
3. Test security policy	☐	✔
User Education and Accountability		
1. Add security training to employee on-boarding	☐	✔
2. Educate staff about what's in the policy and where to find it	☐	✔

Checklist

HarborOne VOYAGE FOR BUSINESS

Cyber Security - Explanations

Password Integrity

You need a password policy for accessing company systems. For example, require passwords that include letters, numbers, symbols, case sensitivity and length. You could include a policy on how often passwords must be changed. This can often be enforced using software settings.

Multi-Factor Authentication (MFA)

Multi-factor Authentication (MFA) is an authentication method that requires users to provide additional credentials to gain access to an application, online account, or a network. It usually involves a special code being sent to the user's phone either via text message or an application on their phone.

Record how you will use MFA in your business. Adding Multi-Factor Authentication to your accounts helps protect against many of the biggest threats to your data such as phishing attacks, brute-force attacks and password reuse.

Email Security

Lock your email so only authenticated users can send emails from your domain. Email can be hacked to send spam that appears like emails sent from your email accounts. Using spam filters, quarantines and the correct SPF, DKIM and DMARK records in your domain setup can all help secure your email. If you use third-party services for email (for example, email newsletters, forms on your website, etc.) then adding these records can also improve deliverability.

These records can be found in your domain settings. If you cannot do this yourself, consult a domain expert to check these for you.

Consider using an email monitoring service that can check if your emails are being delivered and whether anyone is trying to use your email address to send phishing emails.

Secure Wi-Fi

Make sure your networks are secured with complex passwords to prevent anyone hacking in from outside your business. If you offer Wi-Fi access for your customers, this should be on a separate network from your internal systems.

Systems Access

Protecting your systems (computers and networks) is crucial to protect your business and customers' information. Restrict who is allowed access to your systems and where possible, use access privilege settings on hardware and software (for example, administrator, operator, editor, etc). Consider locking cabinets, password protecting computers and installing security cameras. anti-virus and firewall software should be installed to protect against cyber threats.

Regular Backups

It's essential to have a system for your backups and regularly test them. Decide if you'll use cloud-based or on-premise backups and data storage. The frequency of backup you choose depends on your business (for example if you do many transactions every hour, you may need to back up in real time, but if you only have a few changes each day, then a daily backup may be ok.) Backup systems should be automated and well protected with passwords and MFA. If you have physical backups, make sure that you keep a copy off site in case of a fire or natural disaster.

Security Policies

Assign a person to manage your security policies. Document requirements (like those in this plan) that keep your information and employees safe. Test and implement.

User Education and Accountability

Cyber security breaches usually begin by errors made by people within the business. Your employees should know your security policies and why they exist. Store policies in a central place that is accessible to all employees.

If you found this article useful, visit voyage.harborone.com for business advice, tools and templates. Topics include business recovery, improving cash flow, growing sales and succession. Plus access free business plan and cash flow templates, calculators and checklists.