Cyber Security Health Check

Level 1 • Policies & Procedure

Securing your business.

0330 174 9996
info@start-digital.co.uk
start-digital.co.uk

Start Digital

Ver. 2.1

What is This Document?

What is this document?

This document is a cyber security audit; you will filter through and answer each question to improve your business's cyber security one easy step at a time.

We describe **what to do**, as well as **what not to do**. This is labelled as **Good Practice** and **Bad Practice**. You may find that some of your current practices or behaviours fall in to the **Bad Practice** category. This cyber security audit will be a key part of your cyber security journey, and show you what you are missing to secure and protect your business online.

This document's core topics will help you answer the following sort of questions:

> *How do I avoid losing control of my social media accounts?*
>
> *How do I avoid email breaches?*
>
> *How do I recover compromised accounts? (Social/Email)*
>
> *How can I secure my website?*
>
> *Am I doing well with keeping my data safe?*
>
> *Do I have contingency plans ready in case anything goes wrong with my social media/email/website/data?*

Why these core topics are Important:

This document will cover the core topics listed above, as some of them can be easily overlooked This document will help give you and understanding of your goals and aims regarding these topics. Using the topics covered in this document is a good baseline to help you plan your business's future cyber security plan of action.

What you will achieve by completing this document:

The goal of this document is to get you started on your cyber security journey, no matter how small or big the first steps are, any step in the right direction is important. You may want to refer to this document before and after you've implemented your business's new cyber security policies and procedures.

Performing an Audit

How to Use this Document:

This document is laid out in a very simple user-friendly way, with four core columns to focus on. The four columns are set out for you to follow from left to right in the following way:

1: Do You Have?	2:Yes/No	3: Good Practice	4: Bad Practice
Example Question: Do you have a secure password?		**Example Good Practice** A combination of the below: • Capital Letters • Lower Case Letters • Numbers • Special Characters. • Minimum 12 characters • Long Phrases	**Example Bad Practice:** • Names • Dates • Numbers • Predictable Sequences • Short Single Words • Short Phrases
This is a question to **assess** if you have a **specified cyber security** practice in place Some of these questions may have a simplified version which may be easier to understand.	You will answer with a **Yes/No** in this box	This will be **our recommendation** of what you should do to solve your lack of cyber security labelled as a **Good Practice**. A **Good Practice** is a behaviour that is **identified** as an **industry standard way** of doing particular things.	This is a section where we go over common **Bad Practices**. If any of your **current** behaviours are listed in the **Bad Practice example,** then you should put a **no** in the **Yes/No** box and look at the **Good Practise** for an idea of what you should be doing instead.

How to Use the Total Score Table:

At the end of every module, there is a **Total Score** table. This table is where you **total up** all your **yes/no** answers **for each module** you complete:

Total Score:	*Y:* *N:*	*Notes:*
This is the **total number** of **yes/no** answers in the boxes to the **right**.	This is where you will put the **amount** yes and **no answers** you have **totalled** up per section.	You can use this box for any **additional notes** you want to make for each unit you have covered.

Policies & Procedure

Policies & Procedure - Risk Management:
Most businesses will have documented policies and procedures that are designed to signpost and help you control risk within the business. The control of risk is one of the most important aspects that a business leader must oversee and the following guidelines should help you to implement a framework for good practice.

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have any policies within your business? How are your policies and procedures stored within the business? Are they stored in a single location?		Policies are an important tool for businesses, these can be regarded as rules or guidelines within your business to help guide people within the business. You can group the policies by: • Creating them in a single document(word doc, PDF, etc.) • Having a folder/location to store all policy documents. **Note:** Having a backup of these is also a useful way to make sure you have them.	Not having any policies written out/documented. OR A centralised access point to view the policies
Do you have a password policy?		A password policy is a set of rules for employees that covers the creation, change and use and re-use of any passwords they use in the business. It is a good resource to direct employees to when making/changing passwords. A solid password policy contains: • Password creation rules • Multi factor authentication use • Password managers (if in use) • What not to do with passwords • What to do if the policy is violated • Supporting Documents	Not having guidance/rules on passwords documented.
Do you have an acceptable use policy?		An acceptable use policy can be used internally or externally to show your business's stance on how to use products or equipment. The policy should give an understanding of what is expected from the employee or user when they use the product or equipment. An acceptable use policy usually contains: • Product's use case • What happens when people go against the policy • Who to report violations to • Generalised statement to say it can be updated • What the business expects the product to be used for • Supporting Documents	Not having acceptable use of resources, devices, equipment etc documented.

Policies & Procedure

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have a social media policy?		A social media policy is a way to direct employees on what should and should not be said on the business's social media, and what can be said about the business on their personal social media accounts. A policy also good for outlining social media correspondents and who can access the business social media. A good social media policy contains: • How you want the social media to be used by employees • Who can access or post • Who can reply on social media • Limitations on what can be posted on social media • What can be said about the business on employee's social media • Supporting Documents	Not having any policies written out/documented. OR A centralised access point to view the policies
Do you have a disaster recovery plan?		A disaster recovery plan is a very important document for a business. It doesn't need to be cyber security specific, it can also contain other types of disaster that can occur, such as a natural disaster, often referred to as an "act of god". Your disaster recovery plan is a plan of action that you can use to set out guidelines for how you get back to normal business operation as quickly as possible and reduce the possible panic within the business when a disaster does occur. A disaster recovery plan contains: • Recovery time objective (RTO) • Recovery point objective (RPO) • Hardware and software inventory • How important the inventory is for normal operation • Who is responsible for what in case of a disaster • Site locations of where assets are stored – how stocked up they are • Remote location of backups Staff procedures to get back to normal functionality • Identify sensitive data • Communication plans • Supporting Documents	Not having guidance or rules on how to deal with possible disasters documented in an easily accessible format and location.

Policies & Procedure

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have an email policy?		An email policy is a set of rules that outlines how employees are expected to use their business email accounts, such as outbound and inbound emails, and rules on how sensitive emails are handled. A good email policy contains: • Who must follow the document • What not to do in a business email • What to use business email for • What to do when receiving an email • Email formatting • Supporting Documents	Not having guidance or rules on how you expect your employees to use their business email accounts documented in an easily accessible format and location.
Do you have a remote access policy?		A remote access policy is more relevant than ever, it is a policy which dictate the how, when and where can an employee work from outside of the normal work place, it can also include requirements from the business to be able to do this. A good remote access policy contains: • Who is allowed to work remotely • Who authorises it • What is required for remote access System requirements (version/model) • Software requirement (version/build) • VPN use requirements • Anti-virus • Password protections • Supporting documents	Not having guidance or rules on how you expect your employees to access and business information and or data outside of the main network documented in an easily accessible format and location.
Do you have a data breach response policy?		A data breach response policy can often somewhat overlap with disaster recovery. This is a policy on how your employees should act, who to contact, and who should be involved in the case of a data breach. A good data breach policy contains: • Contact information – who to contact in base of a breach • Access removal • Incident response team • Types of breaches • Example situations, with example solutions to those situations • Recovery • Assessing the current risk of a data breach occurring • Supporting Documents	Not having guidance or rules on how you expect your employees to react and respond to a data breach occurring documented in an easily accessible format and location.

Policies & Procedure

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have an access control policy?		An access control policy outlines how the business dictates access to its various different resources. It also will include ways on how to restrict or reduce access to different resources, data, information and software within the business. A good access control policy contains: • Who can edit people's access • How to keep data secure, physically and online/software • How to determine peoples access, or how strict you want access to be • Who to contact/what to do if there is suspicious activity around data • Supporting documents	Not having guidance or rules on how you expect your employees to use their business email accounts documented in an easily accessible format and location.
Do you have a denial of service response plan?		A denial-of-service (DoS/DDoS) response plan is a plan of action in the case of a denial-of-service attack. This can include what actions you will take throughout the process of a DoS/DDoS attack. This will reduce the need for thinking of steps and solutions in the midst of a high-pressure situation, and allow you to focus on solving the issue rather than wasting time thinking of the steps you are going to take. A good DoS/DDoS attack policy contains: • The nature of attacks • Monitoring • How to Interpret attack data • How/What mitigations to deploy • Supporting documents Key factors to take in to account: • Preparation • Analysis • Mitigation • Wrap-up	Not having guidance or rules on how you expect your employees to access and business information and or data outside of the main network documented in an easily accessible format and location.
Do you have regular staff training?		While having policies themselves is extremely important for a business, not having the proper staff training to explain the requirements and rules of each policy, as well as how to execute them if such a situation arises, is as good as not having any policies set in the first place. This means that staff training is critical in ensuring your policies are effective.	Not having training to explain the existence of, as well as how to use the policies you do have in your business.

Policies & Procedure

Total Score:	Y:
	N:

Notes:

After completing this module of the audit, you should have a better understanding of how to identify and manage risks. You'll also have an idea of what sort of policies you can make to improve your business's security and how to utilise them to your advantage to keep your business efficient and safe.