Cyber Security Health Check

Level 2•Identity & Access Management

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:

> “*What can I do to keep my network secure?*
>
> *How can I understand the big-picture of my network?*
>
> *Do I have the right processes in place to make my network stay secure?*
>
> *Do I have support systems in place in case of a cyber-attack?*
>
> *Am I handling data correctly?*
>
> *Am I keeping an eye on my network where possible?*”

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.

Identity & Access Management

Identity and Access Management

Identity and access management is a good way to limit vulnerabilities from both purposeful and accidental breaches. Identity and access management is a collection of process with the purpose of reducing access or increasing difficulty to access certain part of a network.

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have restrictions on the usage of accounts with administrative privileges		Employees do not need administrator privileges at all times for their normal day to day activities within the business. Set up user accounts that can be used to complete daily tasks without having unnecessary elevated privileges, this limits the severity of potential breaches that could occur. Most employees should have: • An everyday use account (emails, document, etc.) An employee tasked with managing your business's networks and systems: • An everyday use account (emails, document, etc.) • Administrator accounts (Admin tasks only)	Using administrator privileges for every task.
Do you have a Password policy?		A password policy is a set of rules that covers the creation of, change of, use of, and re-use of any passwords within the business. This document acts as a reference point for employees when making changes to passwords. Create a document that 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	Having no guidance or rules regarding passwords documented in the business.
Do you have multi factor authentication enabled where possible?		Certain services have MFA (multi-factor authentication), also known as 2FA (two-factor authentication.) This is an extra layer of security to prove your identity, and a good way to avoid leaked passwords or brute force attacks compromising your accounts. MFA/2FA can be attached to: • Phone numbers • Email • Authentication App	Not using multi-factor authentication when possible.

Identity & Access Management

Do You Have?	Yes/No	Good Practice	Bad Practice
Do you have a policy covering user access rights?		Having a document that details your employee's access rights is important for business efficiency as well as cyber security. Having a comprehensive policy allows you to quickly sort and assign your employees' needs for access to devices and programs. Create a document that outlines: • Who is responsible for assigning employee'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	Having no limits on what your employees or users can do on your network or devices.

Identity & Access Management

Total Score:	Y:
	N:

Notes:

Now that you have completed the Identity and access management module, you should have a much better understanding of your current level of identity and access management, where you're lacking, and the areas where you can make improvements.