Cyber Security Tool Kit

Level 1•Data & Info Security

Securing your business.

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

Start Digital

What is This Document?

What is this document?

This **Level 1 Cyber Security Tool Kit** is a step-by-step guide to help you implement the measures and processes covered in the **Level 1 Health Check**.

Not all fields or groups of boxes will need to be filled in. We expect you to only fill in the ones you plan on implementing based on your health check audit results. You can always go back later to complete any additional modules if necessary.

The **Level 1 Cyber Security Tool Kit** is a *living document*, which means that you will be continually editing and updating the document. Cyber security is an on-going process, and sitting still is not a position you want to be caught in. Most of this document's tasks cannot be completed in a single sitting, or a short period of time. This means you will be coming back regularly to make updates and changes.

Policy Implementation:

Certain topics within the **Level 1 Cyber Security Tool Kit** may be covered by existing policies you have implemented within your business. You may find that you can improve your existing policies with the help of the **Level 1 Health Check** and this **Level 1 Tool Kit**. If your existing policies are working as they should though, rather than repeating yourself, you can add supporting documents to the relevant policies and redirect towards the documents with the necessary information.

What you will achieve by completing this document:

The goal of this document is to support your on-going cyber security journey, no matter how small each step is. Any step you take in the right direction is an important improvement to your business's cyber security, as well as establishing your business's digital culture.

Establishing a digital culture:

Advancements and the reliance on digital technology coupled with classic business models have accelerated business disruption. In an increasingly global marketplace, the pandemic has further accelerated this trend, making the digital transformation critical for a business's success. However, it takes more than just technology and policies; the business leaders must also look at the human side of their organisations.

The culture within the business around the way your employees interact with technology is a significant factor in staying secure, and being successful. Developing a strong digital culture from the top down is an extremely important element to ensuring the policies you develop become second nature to all employees. Without the right culture of behaviour, the policies you implement have limited impact.

This is a document you will regularly refer back to before and after you've implemented your business's new cyber security policies and procedures.

Completing Task Sheets

Completing Task Sheets:

This document's task sheets are laid out in a very simple, user-friendly table format. A task sheet has 2 primary elements: the **topic table**, and the **question** and/or **task box**. Some task boxes may include a **tick box** to indicate you have completed that specific task or full topic.

Topic Table:

This is a table at the start of each module with each topic categorised. Once you have completed a full task, you can tick it off to keep track of the tasks you have carried out.

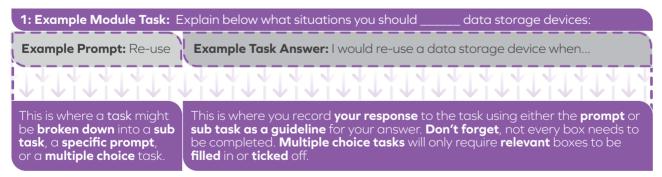| 1: Topic Number	2: Module Topic	2: Tick Box
Example Number: 1	**Example Topic:** Cyber security policy	✓
This is just a simple box to denote the number of topics within a module.	This box names the specific topic of the module you are currently working through.	Tick this box to show you've completed the named topic.

Answer Table:

Answer tables are set out in two different formats: **question boxes** where you are asked specific questions that require specific answers; and **task boxes** where the goal is for you to carry out a specified task, and then mark it as complete when you have finished. Some tasks will be multiple choice, where you choose one task or another.

Question Box:

1: Example Module Question: What processes do you have in place for email safety?
Example Answer: Our current processes are…
This is where the question is asked, and you fill in the lower boxes with your answers.

Task Box:

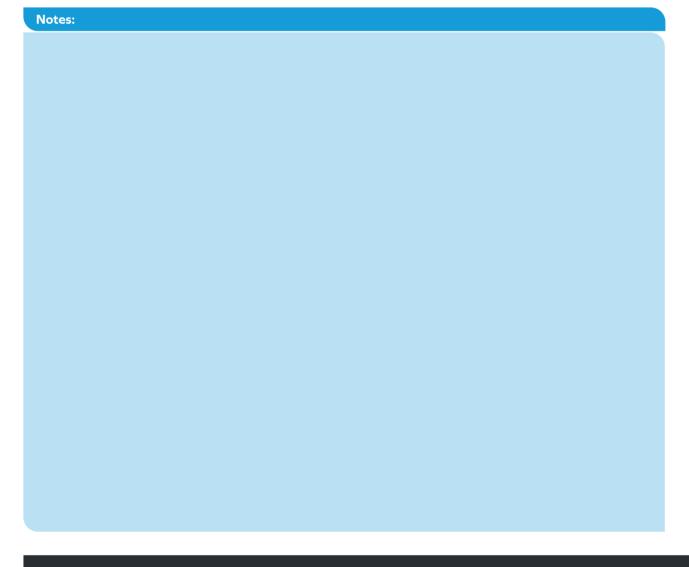| 1: Example Module Task: Explain below what situations you should _____ data storage devices:	
Example Prompt: Re-use	**Example Task Answer:** I would re-use a data storage device when…
This is where a task might be **broken down** into a **sub task**, a **specific prompt**, or a **multiple choice** task.	This is where you record **your response** to the task using either the **prompt** or **sub task as a guideline** for your answer. **Don't forget**, not every box needs to be completed. **Multiple choice tasks** will only require **relevant** boxes to be **filled** in or **ticked** off.

Data and Info Security

Data and Information Security:

Data is an important asset for businesses, and protection of that data needs to be a priority. Data breaches can lead to fines or loss of customer trust, and the overall impact it has on your business can be immense. To avoid such a situation, as well as minimising the damage when one occurs, all businesses are required to implement correct security measures as well as employ staff who are aware of their legal responsibilities when handling data.

Number	Module Topic	✓
1	Backups	
2	Access Control	
3	Encryption	

Module Notes:

You can use this box to add any notes you feel are necessary to help you work through this module.

Notes:

Data and Info Security

1. Backups:

Backups are a very important part of both physical security as well as cyber security. Having reliable backups is an important control that a business must have to prevent long-term damage following a data breach. Backups reduce risks following a ransomware or malware attack, or even accidental deletions. The more frequently a business backs up its critical data, the less downtime there will be, enabling a quicker recovery when there is an incident.

Which types of data are most important, or critical, to your business's operation? Tick all that apply. ✔

- Customer Information
- Employee Information
- Work Documents
- Sales
- Supply Chain Data
- Hardware/Software Inventory Data
- Market Research
- Website Data
- Customer Surveys/Feedback
- Emails

You may hold other types of important data, if so, list them below:

Tick the box once complete.

Password Security

2. Unique Passwords:

Having unique passwords for each account you have increases the safety of all other accounts collectively. If a single account gets breached, the rest remain safe. Unique and secure passwords are difficult to remember, so following task 1 of the password security module will help with completing this task.

How many re-used (not unique) passwords do you have in use within your business?

Change all re-used passwords to a new unique password using the password creation rules below:

- 12 characters minimum
- Caps and lower case
- Numbers
- Special characters (*/'.,£$& etc.)

Tip: if you have more than 5 accounts it is recommended to use a password manager

If you haven't changed a password within the last 6 months, change those as well.

Tick the box once you have completed this topic.

3. Multi-Factor Authentication (MFA):

MFA is a great way to keep secure. Though some find it an inconvenient hurdle in their day to day work-flow, it's become a necessary step in establishing security. MFA requires all login attempts to be authenticated using additional means such as: text, email, or via an app. Make a list of the online services your business uses in the table below:

Online services necessary for the business's day-to-day operations. (do not tick boxes at this stage)	✓

Research how to implement MFA on the services you use above. Tick off each service once completed.

Tick the box once you have completed this topic.

Data and Info Security

2. Access Control:

Access control can be put in place on both systems and networks to restrict access to certain data for users. Access control is an important security procedure that should be implemented on any system or network if it is susceptible to attacks from both outside and inside forces. Access control has a very simple overall purpose: It allows a business to set specific individuals read-write-execute rights to particular files and directories of a system, and/or membership in specified groups and access to those shared folders.

Access Control Service Assessment:

Step 1. Research the access control services in the table below, tick off any that you feel meet the needs of your business. Tick off any that apply, however you will ultimately only choose and use 1.

Access Control Services:

Service:	Cost:	Pros:	Cons:	✓
Kisi	£			
Vanderbilt Industries	£			
ISONAS	£			
Brivo	£			
Honeywell	£			
Johnson Controls	£			
Envoy	£			
Salto	£			
Bosch	£			
HID	£			
Pulse Policy Secure	£			

Other:

Which access control service would you use, and why?

Implementing Access Controls.

Step 2. Implement access control using your chosen service. Go through the steps the service provider gives for your particular service, ensuring you document the process along the way.
Step 3. Nominate someone to be responsible for setting access levels. This could be you, or someone you trust.
Note: Make sure to be conscious about physical access controls, these are covered in other modules.

Using the box below, list the name and contact details of the individual who is responsible for setting access levels.

Tick the box once you have completed this topic.