# Cyber Security Tool Kit

## Level 1•Hardware & Software

Securing your business.

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

Start Digital
Ver.2.1

# 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:**<br>1 | **Example Topic:**<br>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. |

# Hardware and Software

## Hardware and Software Security:

Hardware security protects the physical machine and any peripheral hardware from damage. Software security is the protection of your software from malicious attacks and other security risks.

Hardware risks are generally more common when the hardware itself is particularly outdated, and likewise with software.

This module of the tool kit covers developing your hardware and software digital culture in a way that greatly improves the overall security of your business.

| Number | Module Topic | ✓ |
|---|---|---|
| 1 | Anti-Virus/Anti-Malware Software | |
| 2 | Updating: Systems | |
| 3 | Updating: Applications | |
| 4 | Updating: Drivers and Firmware | |
| 5 | Network Security: Hardware | |
| 6 | Network Security: Virtual Private Networks (VPNs) | |
| 7 | Network Security: Firewalls | |
| 8 | Taking Inventory: Hardware | |
| 9 | Taking Inventory: Software | |

## Module Notes:

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

Notes:

# Hardware and Software

## 1. Anti-Virus/Anti-Malware.

Antivirus, or Anti-malware, is software that protects your devices, such as: your work computer, mobile, and other internet-connected devices from security threats. Some antivirus software uses live protection to stop your computer from being hacked, blocks  malware from running on your devices. Having a robust antivirus running on your systems is an important first step in protecting yourself and your systems from threats.

**Encryption Assessment:**

**Step 1.** Research the anti-virus services in the table below, tick off any that you feel meet the needs of your business. Some services will have specific use cases, so you might end up choosing more than one.

**Anti-Virus/Anti Malware Applications/Services:**

| Service: | Cost: | Pros: | Cons: | ✓ |
|---|---|---|---|---|
| Bitdefender Gravityzone Business Security | £ | | | □ |
| ESET endpoint security | £ | | | □ |
| Avast Business Antivirus Pro Plus | £ | | | □ |
| Sophos Intercept X | £ | | | □ |
| McAfee Total Protection | £ | | | □ |
| Norton Small Business | £ | | | □ |
| AVG Business | £ | | | □ |
| Malwarebites | £ | | | □ |
| Kaspersky | £ | | | □ |

**Other:**

**Which anti-virus/anti malware applications/services did you choose, and why?**

**Implementing Your Chosen Anti-Virus Services and/or Software. Tick off each once complete.**

| | |
|---|---|
| **Step 3.** Purchase your chosen anti-virus service, or services if you have chosen more than 1. | □ |
| **Step 4.** Using the guidelines of the chosen service, install on all of your relevant systems and devices. | □ |
| **Step 5.** Configure on all necessary systems and devices to meet your business's specific needs. | □ |
| **Step 6.** Scan each device/system using the anti-virus software, and remove any known malware. | □ |
| **Tick the box once you have completed this topic.** | □ |

# Hardware and Software

## 2. Updating: Systems.

There is a reason why businesses don't update their software like they should. Many times it's because updating software isn't easy or convenient for business users, this becomes more of an issue for businesses that have thousands of users and computers. However without system updates, the security of your system isn't guaranteed as you aren’t keeping your systems ahead of the most recent, prevalent and damaging security exploits.

**Which operating systems do you have in use across your business?**

**Windows:** List which builds (below) as well as the amount of systems it’s installed on (right box).

**Mac OS:** List which builds (below) as well as the amount of systems it’s installed on (right box).

**Linux:** List which build/distro (below) as well as the amount of systems it’s installed on (right box).

**Task:** Research how to complete the tasks below. Tick each one off as you go.

1. How to enable automatic updates,and or notifications for when there is an update. □
2. How to check your operating system’s build number or version number. □
3. How to perform an update, and updating all systems to the latest available build where possible. □

**Tick the box once you have completed this topic.** □

## 3. Updating: Applications.

You may have heard "vulnerability" being used a lot in recent times, and whilst vulnerabilities are mostly referred to in the context of cyber security, it's a term that applies to any sort of weakness that can be exploited. This makes keeping your applications up to date is now even more important than ever. Typically, vulnerabilities are the result of flaws in the coding process or bugs in software that have allowed hackers to exploit and gain access to areas they shouldn't be able to. This allows them to change or add to the code to perform often malicious functions.

**Application Update Process Assessment.**

**Step 1.** Research the application update management services in the table below, tick off any that you feel meet the needs of your business.

**Software Update Management Applications/Services:**

| Service: | Cost: | Pros: | Cons: | ✓ |
|---|---|---|---|---|
| Glarysoft Software Updater Pro | £ | | | □ |
| Patch My PC Updater | £ | | | □ |
| Iobit Software Updater | £ | | | □ |
| Systweak Software Updater | £ | | | □ |
| Hemidal Free | £ | | | □ |

**Other:**

**Which software update management applications/services did you choose, and why?**

**Task:** Complete the tasks below. Tick each one off as you go.

1. Buy/download chosen software update management application/service. □
2. Install on all relevant devices or systems. □
3. Set up the software to meet your business's needs. □
4. Perform a scan on your systems to assess whether any applications need to be updated. □
5. Update applications according to the results of the update management scan. □

**Tick the box once you have completed this topic.** □

# Hardware and Software

## 4. Updating: Drivers and Firmware.

Keeping your network-connected hardware's drivers and firmware up to date can often be neglected by administrators. Network-connected devices running old drivers or firmware can act as the perfect entry point for an attacker. However, it isn't a straight-forward process. This can be a technical task that might be difficult for your digital lead depending on their experience. The best practice is to only update the drivers and firmware of critical devices or hardware when there are critical security updates for those devices. This is because updating firmware of critical hardware carries the risk of down-time for those inexperienced.

**Application Update Process Assessment.**

Research the driver/firmware update management services in the table below, tick off any that you feel meet the needs of your business.

**Driver/Firmware Update Management Applications/Services:**

| Service: | Cost: | Pros: | Cons: | ✓ |
|---|---|---|---|---|
| System Mechanic Ultimate Defence | £ | | | |
| Outbyte Driver Updater | £ | | | |
| DriverFix | £ | | | |
| Smart Driver Care | £ | | | |
| AVG Driver Updater | £ | | | |
| Driver Easy | £ | | | |
| Driver Genius Platinum | £ | | | |
| Driver Booster | £ | | | |

**Other:**

**Which driver/firmware update management applications/services did you choose, and why?**

**Task:** Complete the tasks below. Tick each one off as you go.

| | |
|---|---|
| 1. Buy/download chosen driver/firmware update management application/service. | |
| 2. Install on all relevant devices or systems. | |
| 3. Set up the software to meet your business's needs. | |
| 4. Perform a scan on your systems to assess whether any drivers or firmwares need to be updated. | |
| 5. Update drivers/firmware according to the results of the update management scan. | |

**Tick the box once you have completed this topic.**

# Hardware and Software

## 5. Network Security: Hardware.

### Wireless:

No matter the size of the business, a network will be used in some capacity. So making sure your network is secure is a must. WiFi is a very easy and common entry point into a network. If someone can gain easy access through unsecured WiFi broadcasts, it can lead to them being able to snoop and search around the whole network to look for other vulnerabilities or devices they can connect to and exploit.

### Wired:

An aspect often overlooked in network security is physical access to a network using ethernet ports. If you have cameras or other devices such as: wireless access points, that are powered by PoE (power-over-ethernet), you have to be careful to make sure they're sited correctly and securely. If a PoE device's port can be easily accessed, there is potential for it to be removed and the ethernet cable used to gain access to the network. Siting them correctly discourages this type of attack, but having correctly configured network access policies in place will limit what someone can see or do, even if they do manage to connect.

**Securing Your Network.**

Research the network hardware in use within your business. Complete the table below, ticking off task as you go. This process is your first step in becoming more security conscious of your business's network.

**Your Business's Network Hardware.** Put the manufacturer and model in the box on the right.

| | |
|---|---|
| What network router do you have? | |
| What network switch do you have? | |
| Do you have wireless access points (WAPs)? | |
| Do you have a server? If so, which model? | |
| Do you have a NAS? If so, which model? | |

**Securing Your Network Hardware.** Complete the network security tasks below. Tick each one off as you go.

1. Go to your device's configuration page. This is done by putting its IP address in to a browser. □
2. Login to the configuration page. The default credentials will be listed on your device's info sticker. □
3. Navigate to the device's administration page, this is often under "advanced settings." □
4. Change your device's login user name and password, ensuring your chosen password is secure. □
5. Enable encryption for devices with WiFi radios. This varies per device, so might require some research. □
6. Look for the SSID settings on your WAPs. This is the name of the WiFI connection you see on devices. □
7. Change the default SSID on wireless access points to one more suitable for your business's needs. □
8. Store all the information/details you have changed within a password manager, or secure notebook. □

**Tick the box once you have completed this topic.** □

# Hardware and Software

## 6. Network Security: Virtual Private Networks (VPNs).

VPNs are commonly used by businesses to protect confidential information and other sensitive data from being stolen or intercepted by an outside party. A VPN creates a secure connection between two networks or devices. This prevents unauthorised monitoring and access to the data transmission between computers or servers by someone else on the same network. A business may use a VPN to keep critical user data secure while using the Internet, to create its own private network, or for remote employees to connect its offices over public or home WiFi connections.

**VPN Services.**

Research the VPN services in the table below. You might find that you have a need for more than one VPN based on the services they offer, tick off any that you feel meet the needs of your business.

**VPN Services:**

| Service: | Cost: | Pros: | Cons: | ✓ |
|---|---|---|---|---|
| Perimeter 81 | £ | | | |
| NordLayer | £ | | | |
| Twingate | £ | | | |
| ExpressVPN | £ | | | |
| Encrypt.me | £ | | | |
| GoodAccess | £ | | | |

**Other:**

**Which VPN service/s did you choose, and why?**

**OPTIONAL: VPN Software installed directly on networking hardware.**

Some more specialised networking hardware allows you to install and configure a VPN service directly on-device. This allows you to blanket apply the VPN service/s to any of the devices connected to that particular piece of network hardware. This is an optional part of the steps in the task table below.

**Task:** Complete the tasks below. Tick each one off as you go.

| | |
|---|---|
| 1. Buy/download chosen VPN service/s. | |
| 2. Install on all relevant devices or systems. | |
| 3. Configure the VPN software to meet your business's needs. | |
| 4. **OPTIONAL:** Install VPN software on any relevant networking devices. | |
| 5. **OPTIONAL:** Configure the VPN software on networking hardware to meet your business's needs. | |
| **Tick the box once you have completed this topic.** | |

# Hardware and Software

## 7. Network Security: Firewalls.

Firewalls are a core part of most networks and devices. They generally work by filtering and or blocking inbound and outbound network connection traffic on a device. Firewalls are a useful tool  that allow granular customisation to fit the user's needs. You can change a firewall setting to be more secure than default, or relax the security on the firewall depending on your needs for a device or network.

**Which type of firewall/s or firewall functions do you need for your business?** Tick all that apply.

Software Firewall - this is often per-device, and will be installed directly on the device. □

Hardware Firewall - this will be a network device that has a firewall as part of its feature set. □

Packet Filtering - this is a security technique, and is available in both hardware and software firewalls. □

**Firewall Services.**

Research the firewall services in the table below. You might find that you have a need for more than one firewall based on the services they offer, tick off any that you feel meet the needs of your business.

**VPN Services:**

| Service: | Cost: | Pros: | Cons: | ✓ |
|---|---|---|---|---|
| SonicWall | £ | | | □ |
| Ubiquity | £ | | | □ |
| WatchGuard | £ | | | □ |
| Cisco NGFW | £ | | | □ |
| Sophos | £ | | | □ |
| OPNSense | £ | | | □ |
| Firewalla | £ | | | □ |
| Palo Alto NGFW | £ | | | □ |

**Other:**

**Did you choose a firewall service/s? If so, which did you choose, and why?**

**Task:** Complete the tasks below. Tick each one off as you go.

1. Buy/download chosen firewall service/s. □
2. Install on all relevant devices or systems. □
3. Configure the firewall software/services to meet your business's specific security needs. □

**Tick the box once you have completed this topic.** □

# Hardware and Software

## 8. Taking Inventory: Hardware.

Taking inventory of hardware devices used within a business is an important process. Knowing what devices you have, where they should be located, their dedicated individual user or department, serial number as well as date of purchase and proof of purchase is useful information to have documented. It allows you to know where a device should be, and could indicate when a device may have been lost or stolen. Keeping the serial number, proof of purchase as well as purchase date can be invaluable for when or if a device goes missing or is stolen. This information is particularly useful to have if you suffer an insured loss, meaning that the claims process can be managed more efficiently.

| Hardware Device | Serial Number | User/Department | Location | Proof of Purchase |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | |
|---|---|---|---|
| Completed On: | | Completed By: | |

Tick the box once you have completed this topic. □

# Hardware and Software

## 9. Taking Inventory: Software.

Taking inventory of software used within your business is useful for keeping a log of what should or should not be on devices. It also allows you to more easily keep track of updates on software without needing a device in front of you. Lastly, taking a software inventory can help with assessing whether there are any gaps in what you need from the current software or software services in use within your business.

**Note:** This is a document you should update at least every 3 months.

| Software/Service | Version Number | User/Department | Device Installed To | Date of Purchase |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| | | | |
|---|---|---|---|
| Completed On: | | Completed By: | |

Tick the box once you have completed this topic. □