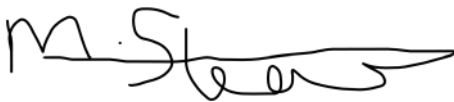


---

# Cyber Essentials Policy

---

Version – 1.0

Name	Title	Signature	Date
Martin Stewart	Author		05/02/2025
Ian Rennell	Sign Off		

System Devices UK All rights reserved, subject to client contract. Information contained in this report may not be published in any form of advertising or other matter without prior agreement of the Managing Director of SDUK

*System Devices UK Ltd is a Limited Company registered in England & Wales. Company Reg No 5474715 VAT No. 866 2857 78*

It is System Devices UK Ltd' prime business objective to provide robust economic electrical, control, communication and information technology systems design, configuration and maintenance support to its Clients. We believe that the fulfilment of this business objective provides Clients with the essential support for compliance with the continuous improvement principles stipulated in the ISO 14000 series of European Standards.

*Note: We make every effort to ensure that this policy conforms to current international laws and best practices and will periodically assess and amend it where necessary to remain compliant.*

## 1 Introduction & Purpose

Data and information are vitally important to us. We all share a responsibility to make sure that it is kept safe and used appropriately. Without due care, it can be misplaced or leaked, which is serious enough without the added difficulty of having to protect it against increasingly proactive and sophisticated attempts at theft.

We have, therefore, adopted this policy to provide the necessary assurance that data and information held and processed by us is treated appropriately to keep it safe, and also to comply with data protection legislation.

This policy is a key component of our overall business management framework and provides the baseline for our information security efforts. The aim of this policy is to set out the rules governing the secure management of data and information by ensuring that all members of the team:

- are aware of and fully comply with the relevant legislation,
- create and maintain a level of awareness of the need for data and information security as an integral part of the day to day business,
- protect data and information that we receive and hold.

## 2 Scope

This policy applies to all data, information, software, applications (i.e. a service used but not downloaded), systems, networks (home, office and others), locations and users of our systems as well as hardware such as laptops, mobile devices, tablets, etc. used to access this, whether owned/ supplied by you, System Devices UK Ltd or otherwise.

### 3 Responsibilities

Ultimate responsibility for data and information security rests with each team member. We cannot ensure that it is secure without you. You are all therefore individually responsible for managing and implementing this policy and related processes and procedures. This is particularly important as our team is so widespread and largely works autonomously.

All of you must, therefore, comply with our data and information security procedures, including the maintenance of data confidentiality, integrity and security. Failure to do so may result in our being unable to work with you and the termination of your contract.

You are also individually responsible for the security of your physical environment where data and information are processed and/or stored. Again this is particularly important as so many of us work outside the office. You are, together with System Devices UK Ltd, responsible for the operational security of the information systems you use.

### 4 Legislation

System Devices UK Ltd is obliged to abide by relevant legislation. It is also each team member's requirement – you may be held personally accountable for any breaches of data or information security for which you are responsible.

### 5 Policy Framework

#### 5.1 Team Contracts

Your contract with System Devices UK Ltd (together with this policy and others) sets out obligations regarding access to the organisation's systems, confidentiality and data security. Security requirements will also be addressed at the induction stage and updated from time to time.

On termination of your contract, all access rights will be removed and all associated accounts will be deleted or disabled, devices will be remote wiped (where possible) and any assets belonging to System Devices UK Ltd must be returned immediately.

#### 5.2 Asset Management

Devices include all computers, laptops, tablets and mobile phones that can access System Devices UK Ltd data and information. It is each team member's responsibility to ensure that these devices meet the following criteria:

- keep devices safe and take care when using them in public spaces,
- devices and operating systems are supported by the supplier/manufacture and get regular fixes (i.e. they are not obsolete),

- all obsolete/ unused/ unsupported software is deleted or disabled,
- anti-malware is installed (where available) and it updates and scans files and websites automatically,
- they must not be modified to remove restrictions imposed by a manufacturer or operator (i.e. 'phones should not be jailbroken),
- software/ applications are only installed from official providers,
- access requires a unique username and password/ passcode
- Full account separation between User and Admin accounts eg Different log-in name and password.
- default passwords are changed for all devices (i.e. from the passwords that are automatically assigned when you first receive them) to a new strong password (at least a minimum of 8 characters and using multi-factor authentication).

### 5.3 Access to Systems

We will ensure that all software/applications used by the team are licensed in accordance with the provider's recommendations and such providers have appropriate terms in their contracts regarding data and information protection. Team members must use unique usernames and strong and unique passwords, which must be changed regularly, to access the software/applications. A respected password manager may be used for this.

When working outside the office you must ensure any router you connect to is protected by a firewall and password protected. Most home internet routers (BT, Virgin, Sky, etc.) have this built in by default – please check regularly.<sup>1</sup> and keep passwords private. Many others, e.g. coffee shops etc. may not be secure so please do not access System Devices UK Ltd data via them unless there is a VPN in place and/or you have enabled your software firewall on your device.

Only team members who have a justified and approved business need shall be given access to certain systems, data and information.

### 5.4 Administrator accounts

Will be regularly reviewed to check the person has a business need for this access,

Must, where possible, have two-factor authentication for access to their accounts enabled.

Must comply to the following complexity rules (at least a minimum of 8 characters and using multi-factor authentication).

## 5.5 Cyber Essentials

We use 'CyberSmart' to obtain and maintain our annual Cyber Essentials certification. It is important that controls to maintain the standard are implemented and reviewed on a regular basis.

## 6 Further Information

Further information and advice on this policy can be obtained from System Devices UK Ltd. Comments and suggestions to improve security are always welcome.