2024

KMP 061 GHL Cyber Essentials Policy

Published Feb 2025
Author: K Nichols
Review Date: Feb 2026
Version 05

Printed on 19 February 2025

Contents

Cyber Essentials Policy

Updated Cyber Essentials Requirements[1]

Version Update: The National Cyber Security Centre (NCSC) released version 3.1 of the Cyber Essentials technical requirements in April 2023. This version includes clarifications and new guidance to address evolving cyber threats. Ensure that your policy reflects these updates.

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, Group Horizon Ltd or otherwise.

3. Responsibilities

Ultimate responsibility for data and information security rests with each employee. 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.

[1] Upcoming Changes: Be aware that version 3.2 of the Cyber Essentials requirements is scheduled to take effect on 28 April 2025. Preparing for these changes in advance will ensure continued compliance.

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 da-ta 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 Group Horizon Ltd, responsible for the operational security of the information systems you use.

4. Legislation

Group Horizon Ltd is obliged to abide by relevant legislation. It is also each employee'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 Group Horizon 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 Group Horizon Ltd assets must be returned immediately.

5.2 Asset Management

Devices include all computers, laptops, tablets, and mobile phones that can access Group Horizon Ltd data and information. It is each employee'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/manufacturer 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, and 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 and using multi-factor authentication

- A minimum password length of at least 12 characters, with no maximum length restrictions
- A minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.

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. Employees 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.1 and keep passwords private. Many others, e.g. coffee shops etc. may not be secure so please do not access Group Horizon Ltd software or data via them unless there is a VPN in place and/or you have enabled your soft-ware firewall on your device.

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

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 have a comply to the following complexity rules: -
  - A minimum of 8 and using multi-factor authentication
  - A minimum password length of at least 12 characters, with no maximum length restrictions
  - A minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.

To check, open a web browser and type into the URL "192.168.0.1". This will direct you to your home router login page. The username and password should be on the back of your router. Go to the settings and configurations and ensure "Firewall" is turned on/enabled.

Default Router IP Addresses Vary

192.168.0.1 is a common default gateway for many routers, but other common IPs include:

192.168.1.1 (used by many Linksys, Netgear, and TP-Link routers)

192.168.1.254 (some BT and Plusnet routers)

192.168.100.1 (some ISP-specific routers)

How to confirm the router's IP:

On Windows: Open Command Prompt (cmd), type ipconfig, and look for Default Gateway.

On Mac/Linux: Open Terminal and type ip route | grep default.

Default Login Credentials Are a Security Risk

Many routers still print their default username/password on the back.

Change these immediately to prevent unauthorised access.

Use a strong password (12+ characters with a mix of letters, numbers, and symbols).

Checking and Enabling Firewall Settings

Once logged in:

2. Look for Security or Firewall settings.
3. Ensure Firewall is enabled.
4. If available, enable intrusion detection and denial-of-service (DoS) protection.

Additional Security Steps

- Firmware Updates: Ensure the router's firmware is up to date.
- Disable Remote Management: Prevents external access to router settings.
- Use WPA3 or WPA2 Encryption: Avoid WEP, as it's insecure.
- Change Wi-Fi SSID & Password: Default names can reveal router models, making them easier to exploit.

The 192.168.0.1 method still works, but not for all routers.

The security of routers has evolved, so it's critical to change default credentials and enable strong security settings.

5.4 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. Remote Work Considerations

Given the increase in remote working, it's crucial to address the security of home networks and personal devices:

- **Home Network Security**: Advise employees to secure their home Wi-Fi networks with strong passwords and encryption.
- **Use of Personal Devices**: If personal devices are used for work purposes, ensure they meet GHL's security standards, including up-to-date anti-malware software and secure configurations.

7. Cloud Services

With the growing reliance on cloud services:

- **Cloud Configuration**: Ensure that cloud services are configured securely, adhering to the principle of least privilege and implementing MFA.
- **Data Protection**: Regularly review data stored in the cloud to ensure compliance with data protection regulations and GHL policies.

8. Policy Maintenance

- **Regular Reviews**: Schedule periodic reviews of the Cyber Essentials Policy to incorporate the latest cybersecurity practices and address emerging threats.
- **Training and Awareness**: Provide ongoing training for employees to keep them informed about current cyber threats and the GHL's security policies.

9. Further Information

Further information and advice on this policy can be obtained from the Managing Director. Comments and suggestions to improve security are always welcome.