

FREE TEMPLATE FOR SMALL BUSINESSES

Cyber Security Policy Template

A 12-section IT security policy for organisations without a security team, mapped to the five Cyber Essentials controls

Version October 2026

Published by Sovereign Secure Ltd, sovereignsecure.co.uk

Help +44 161 523 5276 | contactus@sovereignsecure.co.uk

Editable version [Word document \(.docx\)](#)

About this template

What it is	A free cyber security policy template for small and medium-sized organisations. Its 12 short sections set the rules for accounts, passwords, devices, software updates, firewalls, malware protection, data, incidents and suppliers. It accompanies our template page at sovereignsecure.co.uk/cyber-security-policy-template/ .
What is inside	Part A: the cyber security policy Part B: how each section maps to the five Cyber Essentials controls Part C: staff acknowledgement record Part D: checks before you apply for Cyber Essentials
Version	October 2026. Sections 4 to 9 follow the NCSC Requirements for IT Infrastructure v3.3, the current Cyber Essentials standard.
Licence	Free to use and adapt within your organisation.
Not a certificate	A policy supports Cyber Essentials certification but does not guarantee it. The assessment checks how your devices, accounts and cloud services are actually set up, not what the policy says.
Getting help	Sovereign Secure Ltd is an IASME-licensed certification body for Cyber Essentials and Cyber Essentials Plus. Test your readiness with our free check at sovereignsecure.co.uk/cyber-essentials-readiness-check/ , or call +44 161 523 5276.

How to use this template

- Edit the [Word version](#), or copy Part A into your own document. Replace everything in **[square brackets]** and delete anything that does not apply.
- Numbers in square brackets, such as **[12]** characters or **[5]** minutes, are suggestions. Change them only to values that still meet the Cyber Essentials requirements.
- Keep it short. A few pages of plain rules people can follow is enough for most small businesses.
- Delete these instructions and the Sovereign Secure footer before you issue the policy.

Put the policy into practice

1. **Check the rules against reality.** If MFA is not on everywhere yet, fix that first.
2. **Approve it.** A director signs and dates it.
3. **Brief your team** and ask each person to confirm they have read it, using the record in Part C.
4. **Diary the review**, and update the policy after any new cloud service, IT provider or incident.

If personal data is in scope, the policy also helps show the appropriate security that UK GDPR expects; the [ICO's guide to data security](#) explains what it looks for.

Part A: Cyber security policy template

Guidance: Replace everything in [square brackets] and remove anything that does not apply. Sections 4 to 9 follow the NCSC Requirements for IT Infrastructure v3.3 (nccsc.gov.uk/cyberessentials/resources).

[Organisation name] Cyber Security Policy

Document control

Version	Owner	Approved by	Approval date	Next review	Classification
[x]	[policy owner]	[name, role]	[date]	[date]	[Internal]

1. Purpose and scope

- This policy sets out how [Organisation name] protects its information, its systems and the personal data it holds.
- It applies to all staff, directors, contractors and volunteers, and to every device, account and cloud service used for our work, including personal devices that access company email or data.
- [Policy owner] owns this policy, approved by [director name] on [date].

2. Roles

- [Policy owner] keeps this policy up to date and makes sure it is followed.
- [IT lead or IT provider] manages devices, accounts and security settings in line with it.
- Everyone it covers must follow it and report anything that looks wrong.

3. Acceptable use

- Company devices, email and accounts are for work. [Limited personal use is allowed / is not allowed.]
- Do not install software, browser extensions or apps that [IT lead] has not approved.
- Never share your login details, including with colleagues or anyone claiming to be from IT.

4. Accounts and access

- Accounts are created only after approval by [role]. Everyone has their own account; shared logins are not allowed.
- People get access only to the systems and data their role needs.
- Administrator accounts are separate from everyday accounts and are used only for admin tasks, never for email or web browsing.
- Accounts are disabled by [the person's last working day], and access is removed when someone changes role and no longer needs it.
- [IT lead] reviews all accounts, including admin and supplier accounts, every [three months].

5. Passwords and multi-factor authentication

- Multi-factor authentication (MFA) is switched on for every cloud service and for any other service that offers it.

- Passwords are at least [12] characters, or at least 8 where MFA is on. There is no maximum length and no forced regular changes.
- Use a different password for every work account. We recommend [password manager] and three random words.
- Change a password straight away if you think someone else knows it, and tell [IT lead].
- Accounts lock after no more than 10 failed attempts, or allow no more than 10 guesses in 5 minutes.

Guidance: Our [Cyber Essentials password policy](#) guide explains each rule, including the option of 8 characters with a block list of common passwords.

6. Devices and secure configuration

- Only devices approved by [IT lead] may access company data, and each is recorded in our device list.
- Before use, default passwords are changed, auto-run is switched off and unused software, accounts and services are removed.
- Devices lock after [5] minutes and need a password or PIN of at least 6 characters, or a fingerprint or face, to unlock. They lock out, or slow down guessing, after no more than 10 wrong attempts.
- Personal devices may access [company email / named apps] only if they meet sections 5 to 9. If they cannot, they must not be used for work.
- Report a lost or stolen device to [IT lead] immediately so it can be locked or wiped.

7. Software updates

- All software is licensed and supported by its vendor. Unsupported software is removed, or isolated on a network with no internet access.
- Automatic updates are switched on wherever possible.
- Updates the vendor rates critical or high risk, updates fixing a vulnerability with a CVSS v3 score of 7 or above, and updates released without a severity rating are installed within 14 days of release. This includes operating systems, applications, browser extensions and router and firewall firmware.

8. Firewalls and remote working

- Every office internet connection sits behind a firewall or router whose default admin password has been changed.
- Remote admin access to firewalls and routers stays off unless there is a documented need and MFA, or an IP allow list with a strong password, protects it.
- Inbound connections from the internet are blocked by default. Any inbound rule is approved by [IT lead], recorded with the business reason and removed when no longer needed.
- Laptops keep their built-in firewall switched on, especially at home and on public wifi.

9. Malware protection

- Windows and Mac computers, including servers, run [anti-malware product], updated as the vendor recommends and set to stop malware running and block connections to known malicious websites.
- Phones and tablets run only apps on [our approved app list], installed from the official app store and managed through [device management tool].
- Never switch malware protection off. If it blocks something you need, ask [IT lead].

10. Data, email and backups

- Company data is stored only in [\[approved services\]](#). Do not forward work email or files to personal accounts.
- Laptops and phones use [\[built-in device encryption\]](#).
- Treat unexpected requests for payments, bank detail changes, passwords or MFA codes as suspicious, and check by phone on a known number.
- [\[IT lead\]](#) backs up [\[named systems\]](#) [\[daily\]](#), keeps at least one copy separate from our main systems and tests a restore every [\[three months\]](#).

11. Reporting incidents

- Report straight away to [\[name, phone and email\]](#) if you click a suspicious link, lose a device, notice unusual account activity or send data to the wrong person.
- Nobody is blamed for reporting promptly; delay makes incidents worse.
- [\[Policy owner\]](#) decides next steps, including whether a personal data breach must be reported to the ICO. Where it must, we report without undue delay and, where feasible, within 72 hours of becoming aware of it.

12. Suppliers, review and breaches of this policy

- Suppliers who manage our IT follow sections 4 to 9 for any accounts they use on our behalf.
- Suppliers who handle our data are asked for evidence of their security, such as a Cyber Essentials certificate.
- This policy is reviewed at least every 12 months and after any significant change or incident. Everyone it covers confirms they have read it.
- Breaching this policy may lead to disciplinary action.

Guidance: For what happens after an incident is reported, use our [incident response plan template](#).

Part B: How the policy maps to Cyber Essentials

Cyber Essentials checks five technical controls: firewalls, secure configuration, security update management, user access control and malware protection. Sections 4 to 9 cover all five. The other sections are not Cyber Essentials controls, but customers, insurers and tender questionnaires routinely ask about them.

Section	What it sets out	Cyber Essentials control
1. Purpose and scope	People, devices and cloud services covered	Scope
2. Roles	Who owns the policy and who manages IT	Not a CE control
3. Acceptable use	What company IT may be used for	Not a CE control
4. Accounts and access	How accounts are approved, limited and removed	User access control
5. Passwords and MFA	Password length and MFA	User access control
6. Devices and configuration	Approved devices, screen locks and personal devices	Secure configuration
7. Software updates	Supported software and the 14-day rule	Security update management
8. Firewalls and remote working	Office routers, home working and public wifi	Firewalls
9. Malware protection	Anti-malware and approved apps	Malware protection
10. Data, email and backups	Where data lives, payment scams and backups	Not a CE control (backups are recommended)
11. Reporting incidents	What to report, to whom and how fast	Not a CE control
12. Suppliers and review	IT providers and review dates	Partly: accounts your IT provider uses are in scope

Part C: Staff acknowledgement record

Section 12 asks everyone the policy covers to confirm they have read it. Record each confirmation here, or in your HR system, and repeat it after every review.

Name	Role	Policy version	Date read	Signature or confirmation

Part D: Checks before you apply for Cyber Essentials

Cyber Essentials certifies controls, not documents. Before you apply, confirm that:

- **MFA is on for every cloud service that offers it.** Under the Danzell question set (v3.3, in force since 27 April 2026), a cloud service without MFA where the service offers it fails the whole assessment on its own.
- **High-risk and critical updates are installed within 14 days.** A missed high-risk or critical update also fails the whole assessment on its own, so check section 7 is true on every in-scope device.
- **A documented process sits behind the answers that need one**, such as how new accounts are approved and the business reason recorded for each inbound firewall rule.
- **Sections 4 to 9 are true everywhere they apply**, including home workers' laptops, phones and any personal devices that access company email or data.

Work through our Cyber Essentials checklist at sovereignsecure.co.uk/cyber-essentials-checklist/, then confirm what your certificate should cover with our free scoping questionnaire at sovereignsecure.co.uk/cyber-essentials-scoping-questionnaire/. Cyber Essentials packages start at £320 + VAT.