CLOUDSWITCHED

FREE RESOURCE — POLICY TEMPLATE PACK

Cyber Essentials Policy Template Pack

Ten ready-to-personalise information security policies aligned to the UK Cyber Essentials scheme. Drop in your company name, set the owner, approver, dates and version, sign the register and put each policy in the hands of whoever has to follow it. Tick what is in scope, type in the rest.

10	CE	100+	Sign
POLICY TEMPLATES INCLUDED	ALIGNED TO CYBER ESSENTIALS	FILLABLE PLACEHOLDERS	TYPE, TICK AND SIGN-OFF

ACCESS CONTROL · PATCHING · MALWARE · INCIDENT RESPONSE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this pack

This pack contains ten policy templates that together cover the control areas required for UK Cyber Essentials — firewalls and boundary protection, secure configuration, user access control, malware protection, security update management — plus the supporting policies an assessor and most customers will also expect to see: acceptable use, password management, mobile / remote working, backup and incident response.

Each policy is written as a one-page template. To personalise:

- ☐ **Tick the policy clauses that apply** to your organisation. Leave any that genuinely do not apply unticked — do not delete them. Assessors expect to see what you considered and rejected, not just what you kept.
- ☐ **Type your company name, document owner, approver, effective date, review date and version** into the document control block at the bottom of each policy.
- ☐ **Sign the policy register** on page 13 once all ten policies have been reviewed and approved by your senior leadership.

> **REPLACE, DO NOT DELETE**
>
> Wherever you see **[Company]**, **[role]**, **[N days]** or a similar bracketed placeholder, replace it with your specific value. Do not delete the clause — if the requirement does not apply, leave the placeholder untouched and add a short note in the register explaining why.

The ten policies

- **01 Information Security Policy** — the umbrella policy that sets the security objectives.
- **02 Acceptable Use Policy** — what staff can and cannot do with company systems.
- **03 Access Control Policy** — joiners, movers, leavers and privilege management.
- **04 Password Policy** — password rules, MFA and credential storage.
- **05 Patch & Update Management Policy** — how updates are applied and verified.
- **06 Malware Protection Policy** — anti-malware controls and incident triggers.
- **07 Firewall & Boundary Protection Policy** — perimeter and host firewalls.
- **08 Mobile & Remote Working Policy** — laptops, phones and home offices.
- **09 Backup & Recovery Policy** — backup cadence, retention and restore tests.
- **10 Incident Response Policy** — detect, contain, recover, report.

01

Information Security Policy

Purpose. This policy sets out [Company]'s overarching commitment to protecting the confidentiality, integrity and availability of information and the systems that process it. It is the parent policy under which every other policy in this pack sits.

Scope — applies to:

- **All employees, contractors, temporary staff and third parties** who access [Company] information or systems.
- **All devices — company-owned and BYOD** — used to handle company data, on or off the corporate network.
- **All information assets** in any form (electronic, paper, voice) at every stage of the lifecycle.

Policy statements

- **Confidentiality.** Information classified as Confidential or Restricted must only be accessible to authorised individuals with a documented business need.
- **Integrity.** All systems must protect data against unauthorised modification through access control, logging and change management.
- **Availability.** Business-critical systems must meet the recovery objectives defined in the Backup & Recovery Policy.
- **Accountability.** All users are accountable for activity performed under their account. Shared accounts are prohibited.
- **Continuous improvement.** This policy and supporting policies are reviewed at least annually, after any major incident and when the business materially changes.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

02

Acceptable Use Policy

Purpose. This policy defines how [Company] employees, contractors and third parties may use company-provided devices, accounts, networks and data. The aim is to protect the business from misuse, data loss and reputational harm.

Scope — applies to:

- **All users** with a [Company] user account or access to [Company] systems.
- **All company-provided endpoints** — laptops, desktops, mobile phones, tablets, removable media.
- **Personal devices (BYOD)** when used to access [Company] email, files or other company data.

Policy statements

- **Business purpose.** Company systems are provided for business use. Reasonable personal use is permitted provided it does not interfere with work or breach this policy.
- **Prohibited activity.** Users must not access, store or transmit unlawful content, disable security controls, install unauthorised software or share credentials.
- **Data handling.** Company data must only be stored in approved repositories. Personal email, personal cloud storage and unencrypted USB drives are not approved.
- **Monitoring.** Activity on [Company] systems may be logged and reviewed for security and operational purposes, in line with applicable law.
- **Disciplinary action.** Breach of this policy may result in disciplinary action up to and including dismissal, and where applicable referral to law enforcement.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

03

Access Control Policy

Purpose. This policy ensures that access to [Company] information and systems is granted only on a least-privilege, need-to-know basis, and that joiners, movers and leavers are handled consistently — the single largest source of access-related findings at Cyber Essentials assessment.

Scope — applies to:

- **All identities** — employees, contractors, service accounts, third-party vendors.
- **All systems** processing [Company] data — on-premise, cloud (M365, Google Workspace, AWS, Azure) and SaaS.
- **All access types** — interactive, programmatic (API keys), remote (VPN, ZTNA) and physical (door codes, smart cards).

Policy statements

- **Joiners.** New accounts are provisioned only after a documented request from [role] is approved. Access is granted to the minimum required role.
- **Movers.** When a user changes role, old permissions are removed before new permissions are added — not simply accumulated.
- **Leavers.** Accounts must be disabled within [N hours, typically 24] of the user's departure. MFA tokens, physical credentials and hardware are reclaimed.
- **Privileged access.** Administrator rights are held by named individuals using separate admin accounts. Day-to-day work is never performed as administrator.
- **Reviews.** Access lists are reviewed at least quarterly for standard users and monthly for privileged accounts. Anomalies are remediated within [N days].

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

04

Password Policy

Purpose. This policy defines the rules for creating, storing and managing passwords and credentials used to access [Company] systems. It aligns to NCSC password guidance and the Cyber Essentials user-access control requirements.

Scope — applies to:

- **All user accounts** on [Company] systems — standard, administrative and service.
- **All authentication mechanisms** — passwords, MFA tokens, SSH keys, API keys, certificates.
- **All locations** where credentials are stored — password managers, secret stores, vaults.

Policy statements

- **Minimum length.** User passwords must be at least 12 characters. Administrative and service accounts must be at least 16 characters.
- **MFA.** Multi-factor authentication is enforced on all cloud services, email, VPN, remote access and all privileged accounts. Hardware MFA is preferred for administrators.
- **No reuse.** Passwords must not be reused across systems or shared between users. Compromised passwords are changed immediately.
- **Storage.** Credentials must be stored in the approved password manager [tool name]. Plain-text storage in documents, spreadsheets or chat is prohibited.
- **Default credentials.** Vendor default passwords are changed before any system enters production. A record is kept of the change.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

05

Patch & Update Management Policy

Purpose. This policy defines how [Company] keeps operating systems, applications, firmware and security tools up to date. Cyber Essentials requires that high-risk and critical patches are applied within 14 days — this policy makes that the default, not the exception.

Scope — applies to:

- **All endpoints** — desktops, laptops, mobile devices, servers.
- **All applications** that process [Company] data, including browsers, productivity suites and SaaS clients.
- **All network and security infrastructure** — firewalls, switches, access points, EDR, MDM.

Policy statements

- **Critical patches** (CVSS 9+ or vendor-rated critical) are applied within 14 days of release. Where a patch cannot be applied, a documented compensating control and exception is recorded.
- **High-risk patches** (CVSS 7–8.9) are applied within 30 days of release.
- **Automatic updates** are enabled on endpoints, browsers and operating systems where the vendor supports it.
- **End-of-life software** is identified and replaced or isolated before the vendor support date. No unsupported software is permitted in production.
- **Verification.** A monthly patch-compliance report is produced from [tool, e.g. Intune, WSUS] and reviewed by [role]. Exceptions are tracked to closure.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

06

Malware Protection Policy

Purpose. This policy defines the controls [Company] applies to detect, prevent and respond to malicious code — including viruses, ransomware, spyware and supply-chain implants. It satisfies the Cyber Essentials malware-protection control objective.

Scope — applies to:

- **All endpoints** handling [Company] data, including BYOD and remote workers.
- **All servers and virtual machines** in on-premise and cloud environments.
- **All email and web traffic** into and out of the corporate network.

Policy statements

- **Endpoint protection.** Approved anti-malware / EDR is installed, centrally managed and updated on every endpoint within scope. Tampering with the agent is prohibited.
- **Email filtering.** Inbound email is filtered for malware, phishing and malicious links. Suspicious attachments are sandboxed before delivery.
- **Application allow-listing.** Where supported, only approved applications may execute on production endpoints. Users may not install unapproved software.
- **Detection & response.** Malware alerts are routed to [tool/queue] and acknowledged within [N minutes]. Confirmed infections trigger the Incident Response Policy.
- **User awareness.** All staff complete phishing and malware awareness training annually and after any major change in threat landscape.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

07

Firewall & Boundary Protection Policy

Purpose. This policy defines how [Company] controls traffic between its internal networks and the internet, and between segments of the internal network. It covers boundary firewalls, host-based firewalls and cloud security groups.

Scope — applies to:

- **All boundary firewalls** at every office, data centre and cloud network edge.
- **All host-based firewalls** on endpoints and servers, including remote workers using corporate or BYOD devices.
- **All cloud network security groups** — AWS Security Groups, Azure NSGs, GCP firewall rules.

Policy statements

- **Default-deny.** Inbound traffic from the internet is denied by default. Each opened port is documented with a business justification and review date.
- **No default passwords.** Firewall administrative interfaces use unique, strong credentials and MFA. Vendor defaults are removed before production.
- **Admin access.** Administrative access to firewalls is restricted to named users from trusted networks. All administrative actions are logged.
- **Segmentation.** Guest, IoT and untrusted networks are segregated from the corporate VLAN. East-west traffic is restricted to documented flows.
- **Reviews.** Firewall rule sets are reviewed every six months. Unused rules are removed. Firmware is updated on the schedule defined in the Patch Policy.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

08

Mobile & Remote Working Policy

Purpose. This policy sets the security expectations for [Company] staff using mobile devices, working from home or working from another non-office location. It complements the Acceptable Use and Access Control policies.

Scope — applies to:

- **All company-issued mobile devices** — phones, tablets, laptops, hotspots.
- **Personal devices used for work** under any approved BYOD arrangement.
- **All remote-working locations** — home offices, hot-desks, co-working spaces, travel.

Policy statements

- **Device hardening.** Mobile devices are enrolled in MDM ([tool]). Disk encryption, screen-lock, automatic updates and remote-wipe are enforced.
- **Network use.** Public Wi-Fi may only be used in conjunction with the corporate VPN / ZTNA. Home networks must use unique, strong router admin credentials.
- **Physical security.** Devices must not be left unattended in public places or in plain sight in unattended vehicles. Loss or theft must be reported within [N hours].
- **Confidentiality in public.** Confidential information must not be discussed or displayed where unauthorised individuals could overhear or observe.
- **Return.** All company devices and data must be returned to [Company] on leaving employment or at the end of the engagement, per the Access Control Policy.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

09

Backup & Recovery Policy

Purpose. This policy defines how [Company] backs up its data and verifies that backups can be used to restore service. An untested backup is a guess — this policy makes restore testing routine, not a once-a-year fire drill.

Scope — applies to:

- **All production data** required to operate the business — file servers, databases, SaaS data, code repositories.
- **Microsoft 365 / Google Workspace data** — email, calendar, OneDrive/Drive, SharePoint/Shared Drives, Teams.
- **Endpoint user data** for users not synced to cloud storage by default.

Policy statements

- **3-2-1.** Three copies of data, on two different media, with at least one offsite or in immutable cloud storage.
- **Cadence.** Critical systems are backed up [daily / hourly]. Recovery Point Objective is [N hours]. Recovery Time Objective is [N hours].
- **M365 / Workspace backup.** Cloud productivity data is backed up by a third-party solution ([tool]). Native retention is not considered a backup.
- **Restore tests.** A sample restore is performed every [quarter / month] and recorded. At least one full disaster-recovery exercise is run annually.
- **Protection.** Backups are encrypted at rest and in transit. Backup credentials are held in the vault and access is restricted to [role].

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

10

Incident Response Policy

Purpose. This policy defines how [Company] detects, contains, eradicates, recovers from and reports security incidents. It also defines the obligation to notify the ICO within 72 hours where personal data is at risk.

Scope — applies to:

- **All security events** affecting the confidentiality, integrity or availability of [Company] data or systems.
- **All staff and third parties** — everyone has a duty to report a suspected incident promptly.
- **All channels** — including supply chain, customer-impacting outages and physical security events.

Policy statements

- **Reporting.** Suspected incidents are reported to [channel, e.g. security@company.com] within [N minutes / hours] of discovery. No reprisal for good-faith reports.
- **Triage.** [Role] classifies the incident severity (Sev 1–4) and convenes the response team within the SLA for that severity.
- **Containment.** Affected systems are isolated, credentials rotated and forensic evidence preserved before remediation actions are taken.
- **Notification.** Where personal data is at risk, the ICO is notified within 72 hours. Affected data subjects are notified without undue delay where required.
- **Post-incident review.** A blameless post-incident review is held within [N days]. Actions are tracked to closure and contribute to the next policy review.

COMPANY NAME	DOCUMENT OWNER	APPROVER

EFFECTIVE DATE	REVIEW DATE	VERSION

Σ

Policy register

Record the live version of each policy here. Tick when the policy has been reviewed by the document owner, approved by senior leadership and made available to staff. The register is the single source of truth for what is in force at any given date.

#	POLICY	VERSION	REVIEWED
01	Information Security Policy	_____	☐ Y ☐ N
02	Acceptable Use Policy	_____	☐ Y ☐ N
03	Access Control Policy	_____	☐ Y ☐ N
04	Password Policy	_____	☐ Y ☐ N
05	Patch & Update Management Policy	_____	☐ Y ☐ N
06	Malware Protection Policy	_____	☐ Y ☐ N
07	Firewall & Boundary Protection Policy	_____	☐ Y ☐ N
08	Mobile & Remote Working Policy	_____	☐ Y ☐ N
09	Backup & Recovery Policy	_____	☐ Y ☐ N
10	Incident Response Policy	_____	☐ Y ☐ N

REGISTER CADENCE

The register is reviewed at every quarterly governance meeting and after any incident that triggers a policy change. A revised policy resets the version number on that row, with a new effective date.

Sign-off & next steps

The policies in this pack take effect on the date below, on the authority of the senior leader named below. Use the action lines underneath to capture the three next steps that will turn paper policies into operating reality.

Senior sign-off

01 Signed for and on behalf of [Company] _____

02 Name & role _____

03 Date _____

Top 3 implementation actions

01 _____

02 _____

03 _____

Notes

_____

_____

_____

PACK VERSION _____

EFFECTIVE DATE _____

NEXT REGISTER REVIEW _____

Need help getting Cyber Essentials certified?

Cloudswitched runs Cyber Essentials and Cyber Essentials Plus engagements for UK SMEs — gap assessment, technical remediation, evidence pack and assessor liaison, with a fixed-price plan up front.

info@cloudswitched.com

cloudswitched.com/services/cyber-essentials

CLOUDSWITCHED

CYBER ESSENTIALS & IT SECURITY SERVICES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom