# Cyber Essentials Policy Template Pack

Ready-to-use policy templates to support your Cyber Essentials Plus certification. Customise for your organisation.

| 6 | CE+ | Edit | Free |
|---|---|---|---|
| POLICY TEMPLATES | FULLY ALIGNED | CUSTOMISABLE & EDITABLE | NO COST DOWNLOAD |

## 1 About This Template Pack

Achieving Cyber Essentials Plus certification requires more than just technical controls — it demands documented policies that demonstrate your organisation's commitment to cybersecurity governance. This pack provides **six professionally drafted policy templates** aligned to the CE+ framework and NCSC guidance.

Each template is designed to be **customised for your organisation**. Replace all placeholder fields (shown as [Organisation Name], [Date], [Version]) with your organisation-specific details. Review each section, tailor the statements to match your operations, and have the policies approved by senior management before distributing to staff.

### Templates Included

| # | TEMPLATE | PURPOSE | CE+ CONTROL AREA |
|---|---|---|---|
| 1 | Acceptable Use Policy | Defines acceptable use of IT resources, internet, email, and social media | All Controls |
| 2 | Password Policy | Sets password complexity, rotation, MFA, and account lockout rules | User Access Control |
| 3 | Access Control Policy | Governs role-based access, least privilege, and joiner/mover/leaver processes | User Access Control |
| 4 | Patch Management Policy | Defines patching schedules, testing, and end-of-life software removal | Security Update Mgmt |
| 5 | BYOD Policy | Controls personal device usage, security requirements, and data separation | Secure Config / Malware |
| 6 | Incident Response Plan | Outlines incident classification, escalation, containment, and reporting | All Controls |

**How to Use These Templates**

1. Replace all placeholder fields with your organisation-specific information. 2. Review and tailor each policy to match your operations and risk profile. 3. Have policies formally approved by your senior management or board. 4. Distribute to all staff and obtain written acknowledgement. 5. Schedule annual reviews and update after any significant operational change.

**Important Disclaimer**

These templates are provided as starting points and general guidance. They should be reviewed by a qualified professional to ensure they meet your specific regulatory, legal, and operational requirements. Cloudswitched accepts no liability for the use of these templates without appropriate professional review.

### Before You Begin — Pre-Implementation Checklist

- [ ] Define the **scope** of your CE+ certification (devices, users, networks, cloud services in scope)
- [ ] Confirm who will be the **Senior Responsible Officer** for signing off on all policies
- [ ] Audit your existing policies to identify what can be updated vs. created from scratch
- [ ] Establish a **version control process** for tracking policy changes over time
- [ ] Plan how policies will be **distributed and acknowledged** by all staff
- [ ] Identify your **incident response team** members and their contact details

## Template 1: Acceptable Use Policy

Defines how employees may use organisational IT resources, internet access, email, and social media

**Organisation:** [Organisation Name] **Version:** [Version] **Date:** [Date] **Owner:** [IT Manager / CISO]

### 1. Purpose

This policy establishes the acceptable use of information technology resources at [Organisation Name]. It is designed to protect the organisation, its employees, partners, and clients from harm caused by the misuse of IT systems and data. Inappropriate use exposes the organisation to risks including malware infections, data breaches, legal liability, and reputational damage.

### 2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and third parties who access [Organisation Name]'s IT resources, including but not limited to: computers, laptops, mobile devices, email systems, internet access, cloud services, printers, and telephone systems — whether accessed on-site, remotely, or via personal devices.

### 3. Internet Use

- Internet access is provided primarily for business purposes. Limited personal use is permitted provided it does not interfere with work duties, consume excessive bandwidth, or breach any other policy.
- Users must not access, download, or distribute material that is illegal, offensive, discriminatory, sexually explicit, or promotes violence or hatred.
- Downloading software, browser extensions, or applications from untrusted sources is strictly prohibited without prior written IT approval.
- Streaming services, peer-to-peer file sharing, torrent applications, and VPN/proxy services to bypass filtering are not permitted on organisational devices or networks.
- All internet activity may be monitored and logged in accordance with applicable legislation. Users should have no expectation of privacy when using organisational internet access.

### 4. Email Use

- Email is provided for business communication. Users must not use organisational email for personal commercial activities, chain letters, political campaigning, or mass unsolicited mailings.
- Users must exercise caution with attachments and links from unknown senders. Suspicious emails must be reported to [IT Helpdesk] immediately and must not be forwarded to other users.
- Confidential or sensitive information must only be sent via email when encrypted or through approved secure file-sharing channels.
- Auto-forwarding of organisational email to external personal email accounts is strictly prohibited.
- Users must not impersonate other individuals, use false identities, or send misleading communications when using organisational email systems.

### 5. Social Media

- Personal social media use during working hours must be limited and must not interfere with job performance or productivity.
- Users must not disclose confidential business information, client data, internal communications, or proprietary information on any social media platform.
- When identifying themselves as employees of [Organisation Name], users must conduct themselves professionally and in accordance with company values and brand guidelines.
- Users must not post content that could damage the reputation of the organisation, its clients, partners, or fellow employees.

### 6. Personal Devices

- Personal devices may only access organisational data or systems if enrolled in the organisation's Mobile Device Management (MDM) solution and compliant with the BYOD Policy (Template 5).
- Personal devices must not be connected to the corporate wired or wireless network without prior IT authorisation.
- The organisation accepts no responsibility for the maintenance, support, data loss, or damage to personal devices.

### 7. Responsibilities

All users are responsible for exercising good judgement and complying with this policy at all times. Users must report any suspected security incidents, policy breaches, or suspicious activity to [IT Helpdesk / Security Team] immediately. Line managers are responsible for ensuring their teams are aware of and comply with this policy.

### 8. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. Where illegal activity is suspected, [Organisation Name] reserves the right to report incidents to the relevant law enforcement authorities. Access to IT resources may be suspended immediately pending investigation of any suspected breach.

## Template 2: Password Policy

Establishes requirements for creating, managing, and protecting passwords and authentication credentials

**Organisation:** [Organisation Name] **Version:** [Version] **Date:** [Date]

### 1. Minimum Length & Complexity

- **Minimum length:** All passwords must be at least **12 characters** long. Administrative and privileged accounts require a minimum of **16 characters**.
- **Complexity:** Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters. Alternatively, three-random-word passphrases are acceptable per NCSC guidance.
- **Prohibited patterns:** Dictionary words, sequential characters (abc, 123), keyboard patterns (qwerty), personal information (name, DOB, username), and previously breached passwords are all prohibited.
- **Uniqueness:** Passwords must not be reused across different systems, services, or accounts. The previous 12 passwords may not be reused on the same system.

### 2. Rotation Schedule

- **Standard users:** Passwords must be changed every **90 days**, or immediately if a compromise is suspected.
- **Privileged/admin accounts:** Passwords must be changed every **60 days**.
- **Service accounts:** Passwords must be changed every **180 days** and stored in an approved credential vault.
- **MFA exception:** Where MFA is fully enforced, password rotation may be extended to **annual** in line with current NCSC guidance, as frequent rotation without MFA can lead to weaker password choices.

### 3. Multi-Factor Authentication (MFA)

- MFA is **mandatory** for: all cloud services (Microsoft 365, Google Workspace, etc.), VPN and remote access, remote desktop connections, all administrator and privileged accounts, and any system accessible from the internet.
- **Approved MFA methods:** Authenticator apps (Microsoft Authenticator, Google Authenticator), FIDO2 hardware security keys. SMS-based MFA is permitted only as a temporary fallback and must be migrated to app-based methods within 30 days.
- Users must register at least **two MFA methods** to ensure continued access if one method is unavailable.

### 4. Password Manager Usage

All users are required to use the organisation-approved password manager ([Tool Name, e.g. 1Password, Bitwarden]) for generating and storing credentials. Passwords must never be written down on paper, stored in plain text files, spreadsheets, sticky notes, or shared via email, chat, or messaging applications.

### 5. Account Lockout Policy

- Accounts will be **locked after 10 consecutive failed login attempts**.
- Locked accounts require either a **30-minute timed lockout** or manual unlock by IT support.
- Repeated lockouts on any account must be investigated by IT as a potential brute-force or credential stuffing attack.
- All failed login attempts must be logged and available for security audit review.

## Template 3: Access Control Policy

Governs how access to information systems and data is granted, managed, reviewed, and revoked

**Organisation:** [Organisation Name] **Version:** [Version] **Date:** [Date]

### 1. Role-Based Access Control

Access to all systems and data is granted based on the user's job role within the organisation. Each role has a defined access profile specifying which systems, applications, data, and administrative functions the role requires. Access rights are approved by the user's line manager and provisioned by IT.

### 2. Least Privilege Principle

All user accounts are provisioned with the **minimum level of access** required to perform their job duties and nothing more. Elevated or additional privileges are only granted upon formal documented request, line manager approval, and must be time-limited where possible. Access is reviewed and revoked when no longer needed.

### 3. Administrative Account Rules

- Admin accounts must be **entirely separate** from standard daily-use accounts. Admin accounts must never be used for email, web browsing, or routine work.
- Admin accounts require strong unique passwords (minimum 16 characters) and MFA without exception.
- A **register of all admin accounts** must be maintained by IT, reviewed quarterly, and kept to the absolute minimum number required.
- All administrative activities must be **logged, timestamped, and auditable**.

### 4. Joiners, Movers, and Leavers Process

- **Joiners:** New accounts created only upon approved onboarding request from HR/line manager. Access provisioned according to defined role profile. Accounts must not be created in advance of the start date.
- **Movers:** When an employee changes role, previous access rights must be reviewed and adjusted within **5 working days**. Access from the previous role that is no longer required must be revoked — do not simply add new permissions on top of existing ones.
- **Leavers:** All access must be revoked on or before the employee's last working day. Accounts disabled immediately and deleted within 30 days. All shared passwords known to the leaver must be changed. Hardware must be returned and wiped.

## Template 4: Patch Management Policy

Defines the process for identifying, testing, and deploying software updates and security patches across the organisation

**Organisation:** [Organisation Name] **Version:** [Version] **Date:** [Date]

### 1. Patching Schedule

| SEVERITY | TIMEFRAME | DESCRIPTION & CRITERIA |
|---|---|---|
| CRITICAL | Within 14 days | Actively exploited vulnerabilities (CVSS 9.0+) or those on CISA KEV list. Internet-facing systems prioritised. |
| HIGH | Within 14 days | CVSS 7.0–8.9 with known proof-of-concept exploits or affecting widely-deployed software. |
| MEDIUM | Within 30 days | CVSS 4.0–6.9 without active exploitation. Internal systems and non-critical applications. |
| LOW | Next maintenance window | CVSS 0.1–3.9 with limited risk, no known exploits, and minimal attack surface impact. |

### 2. Third-Party Application Patching

All third-party software — including web browsers, PDF readers, Java, media players, conferencing tools (Zoom, Teams), and productivity suites — must be maintained at the latest stable version. Automatic updates must be enabled where available. Third-party applications are subject to the **same patching timeframes** as operating system updates. A software inventory must be maintained listing all installed applications and their current versions.

### 3. End-of-Life Software Removal

- Software that has reached end-of-life (no longer receiving vendor security updates) **must be removed or replaced** before it becomes unsupported.
- An up-to-date software inventory must be maintained showing all installed software, version numbers, vendor support status, and EOL dates.
- Migration plans must be documented at least **6 months** before any software reaches its EOL date.

### 4. Testing Process

- Critical patches for internet-facing systems may be deployed without extended testing where the risk of exploitation outweighs disruption risk.
- All other patches should be tested on a representative subset of devices before broad deployment where feasible.
- A documented **rollback plan** must exist before deploying major updates to production systems.

### 5. Exception Handling

Where a patch cannot be applied within the required timeframe, a formal exception must be submitted to [IT Manager / CISO] documenting: the reason for delay, risk assessment, compensating controls in place, and planned remediation date. Exceptions are reviewed monthly and must not exceed 90 days. All exceptions must be logged for audit purposes.

## Template 5: BYOD Policy

Controls the use of personally-owned devices for accessing organisational data and systems

**Organisation:** [Organisation Name] **Version:** [Version] **Date:** [Date]

### 1. Device Requirements

- Personal devices must run a **currently supported operating system** receiving regular vendor security updates (current or previous major version only).
- **Full-disk encryption** must be enabled: BitLocker (Windows), FileVault (macOS), native encryption (iOS/Android).
- Screen lock must be configured with **PIN (min 6 digits), password, or biometric**. Auto-lock within 5 minutes of inactivity.
- Devices must not be jailbroken, rooted, or have manufacturer security controls bypassed in any way.

### 2. Security Controls

- Personal devices must be enrolled in the organisation's **MDM solution** ([MDM Tool Name]) before accessing any corporate data or systems.
- **Anti-malware software** must be installed, active, and auto-updating on all Windows and Android BYOD devices.
- All OS and application updates must be installed within **14 days** of release. Non-compliant devices will be automatically blocked from corporate resources.
- A personal firewall must be enabled and active on all BYOD laptops and desktops.

### 3. Data Separation & Remote Wipe Consent

- Corporate data must be stored only in **approved managed applications** (e.g., managed email client, approved cloud storage). Local storage of corporate data on personal device storage is prohibited.
- By enrolling in the BYOD programme, the user provides explicit consent to **remote wipe of corporate data** (selective wipe) upon device loss, theft, or termination of employment.
- Where selective wipe is not technically feasible, a full device wipe may be initiated. Users are strongly advised to maintain personal data backups independently.

### 4. Acceptable Use on Personal Devices

Corporate data accessed on personal devices is subject to the same Acceptable Use Policy as corporate-owned devices. Users must not share access to work applications or data with family members, friends, or any other individual. Work data must not be transferred to personal storage, personal cloud accounts, personal email, or unapproved applications under any circumstances.

> **CE+ Scope Impact**
>
> Any personal device that accesses corporate data is within scope for CE+ and must meet all five technical controls. If compliance cannot be enforced on personal devices, consider excluding BYOD from scope by blocking personal device access to corporate resources entirely.

## Template 6: Incident Response Plan

Outlines how the organisation will detect, classify, respond to, and recover from cybersecurity incidents

**Organisation:** [Organisation Name] **Version:** [Version] **Date:** [Date] **Incident Lead:** [Name / Role]

### 1. Incident Classification (P1–P4)

| LEVEL | SEVERITY | EXAMPLES | RESPONSE TIME |
|---|---|---|---|
| P1 | Critical | Active ransomware attack, confirmed data breach involving personal data, total system/network outage, compromised admin credentials | Immediate (within 1 hour). All incident team members mobilised. |
| P2 | High | Malware detected on multiple devices, suspected data exfiltration, compromised user account with data access, DDoS attack | Within 4 hours. Core incident team activated. |
| P3 | Medium | Phishing email clicked (no confirmed data loss), single device malware (contained), unauthorised access attempt blocked by controls | Within 24 hours. Investigate and remediate. |
| P4 | Low | Phishing email reported (no interaction), minor policy violation, port scan detected, spam increase | Within 72 hours. Log, assess, and address. |

### 2. Escalation Matrix

| LEVEL | FIRST RESPONDER | ESCALATION TO | EXECUTIVE NOTIFICATION |
|---|---|---|---|
| P1 | [IT Manager] | [CISO / MD] | Board / Senior Leadership Team immediately |
| P2 | [IT Team Lead] | [IT Manager] | Managing Director within 4 hours |
| P3 | [IT Support] | [IT Team Lead] | Summary in weekly management report |
| P4 | [IT Support] | As needed if pattern detected | Monthly security summary report only |

### 3. Containment Steps

- **Isolate affected systems:** Disconnect compromised devices from the network immediately. Do not power off — preserve volatile memory for forensic evidence.
- **Disable compromised accounts:** Reset passwords, revoke all access tokens and active sessions. Force MFA re-enrolment for affected accounts.
- **Block malicious indicators:** Add identified malicious IP addresses, domains, URLs, and file hashes to firewall, DNS, and endpoint protection block lists.
- **Activate continuity measures:** If primary systems are unavailable, invoke business continuity procedures and establish alternative communication channels.

### 4. Communication Plan

- **Internal:** Use pre-agreed out-of-band channels (e.g., personal mobiles, WhatsApp group) if corporate email/messaging is compromised. Brief staff as needed without disclosing sensitive investigation details.
- **External:** All public and media statements must be approved by [MD / Communications Lead]. No technical details to be disclosed during active investigation.
- **Client notification:** If client data is impacted, notification must be prepared in coordination with legal counsel. Consider contractual notification timeframes.

### 5. Evidence Preservation

All digital evidence must be handled in a forensically sound manner. Maintain a chain of custody log documenting all access to evidence (who, what, when, why). Create forensic images of affected systems **before** any remediation begins. Preserve all relevant logs: firewall, email gateway, endpoint detection, Active Directory/Entra ID, VPN, and CCTV footage if physical access is suspected.

### 6. Post-Incident Review

A formal post-incident review must be conducted within **5 working days** of incident resolution. Document: root cause analysis, full timeline of events, effectiveness of the response, lessons learned, and specific remediation actions to prevent recurrence. All P1 and P2 reviews must be presented to senior management with documented action items.

### 7. Reporting Obligations

- **ICO notification:** Personal data breaches likely to result in risk to individuals must be reported to the ICO **within 72 hours** of becoming aware of the breach.
- **Data subject notification:** High-risk breaches also require direct notification to affected individuals **without undue delay**.
- **Sector regulators:** Notify relevant sector-specific regulators as required (FCA, NHS Digital, Ofcom, etc.).
- **Law enforcement:** Report to Action Fraud (0300 123 2040) and NCSC (report.ncsc.gov.uk) for significant cyber incidents.

> **72-Hour ICO Reporting Deadline**
>
> The 72-hour clock starts from when you become **aware** of a personal data breach, not when it occurred. Failure to notify the ICO within this window can result in fines of up to £8.7 million or 2% of global annual turnover under UK GDPR, in addition to any penalties for the breach itself.

## ✓ Implementation Checklist

Track your progress implementing all six policy templates with this comprehensive checklist.

### Policy Customisation

- [ ] Replace all [Organisation Name] fields across every template with your company name
- [ ] Set [Version] numbers and [Date] on all six policies
- [ ] Assign named policy owners and approvers for each document
- [ ] Tailor all policy statements to match your specific operations, technology stack, and risk profile
- [ ] Specify your approved tools: password manager, MDM solution, patch management platform
- [ ] Complete the Incident Response escalation matrix with named contacts and phone numbers

### Approval & Distribution

- [ ] Submit all policies for review by the Senior Responsible Officer or Board
- [ ] Obtain formal written sign-off and record the approval date for each policy
- [ ] Distribute policies to all employees, contractors, and relevant third parties
- [ ] Obtain written acknowledgement from every member of staff confirming they have read and understood each policy
- [ ] Store signed copies securely with full version history and audit trail

### Ongoing Management

- [ ] Schedule annual policy reviews in the company calendar (or more frequently after significant changes)
- [ ] Include all policies in new starter onboarding and induction processes
- [ ] Conduct regular security awareness training aligned to policy content (at least annually)
- [ ] Test the Incident Response Plan at least annually through tabletop exercises or simulated incidents
- [ ] Maintain evidence of policy compliance for your CE+ assessor and any future audits

**Policy Evidence for CE+ Assessment**

While Cyber Essentials Plus is primarily a technical assessment, your assessor may ask to see documented policies as evidence that controls are managed and maintained. Having these policies in place demonstrates organisational maturity and supports the self-assessment questionnaire that precedes the CE+ technical audit.

**Cloudswitched Can Help With**

- ✓ Customising templates for your organisation
- ✓ Gap analysis against CE+ requirements
- ✓ Full CE+ preparation and assessment support
- ✓ Staff security awareness training
- ✓ Ongoing policy review and maintenance
- ✓ Vulnerability scanning and remediation

**Our CE+ Packages Include**

- ✗ Pre-assessment vulnerability scanning
- ✗ Policy and documentation review
- ✗ Technical controls gap analysis
- ✗ Guided remediation support
- ✗ Assessment coordination with CB
- ✗ Post-certification maintenance plan

**Need Help Implementing These Policies?**

Cloudswitched provides end-to-end Cyber Essentials Plus certification support — from policy creation to successful assessment.

www.cloudswitched.com/services/cyber-essentials

info@cloudswitched.com