

CYBER SECURITY POLICY

POLICY — COMPANY FILE

Accounts, devices, updates, backups, access, logging and incidents — who does what

KD-PQ-CY-013 Rev A0

The National Cyber Security Centre's 10 Steps to Cyber Security divides the job into ten areas: risk management, engagement and training, asset management, architecture and configuration, vulnerability management, identity and access management, data security, logging and monitoring, incident management, and supply chain security. The NCSC aims it at medium to large organisations, and says the principles apply to all. Cyber Essentials is the government-backed scheme built on five technical controls — firewalls, secure configuration, security update management, user access control and malware protection — assessed by verified self-assessment, or with independent technical testing for Cyber Essentials Plus. This policy is organised around those areas in our own words; it is not a certificate and holding it is not certification to either. UK GDPR Article 32 requires security appropriate to the risk for personal data — including the ability to restore access to it in a timely manner after an incident, and regular testing of the measures. Personal data handling and breach reporting are KD-PQ-DP-006; impact assessments for new systems are KD-PQ-DI-012. The law applies across the UK.

CAS v5 Q163 (advisory) — the cyber security policy: what happens in an incident and restoring critical systems from backup (sections 3 and 5), the systems and data that matter and the rules for them (sections 3 and 4), alerts and logs (4.8), work away from the office with its threat table (4.7 and 4.11), and the NCSC 10 Steps position (section 1). A current certificate for Q161 is a separate document; supplier and subcontractor questions (Q165) are in 4.9.

The question numbers are Build UK's; the descriptions are ours. This document records what the business does; the assessment body decides what it accepts. Version 6 of the question set is due on 1 November 2026 and is not yet published — check the numbers against the version you are assessed on. The independence statement is in the footer of every page.

1 THE BUSINESS

COMPANY LOGO add it in your PDF editor, or print and paste it here	BUSINESS NAME	COMPANY NO.	PEOPLE EMPLOYED	VERSION	
	REGISTERED / TRADING ADDRESS	PERSON RESPONSIBLE FOR CYBER SECURITY			
	POLICY DATE	APPROVING DIRECTOR	POSITION	NEXT REVIEW DUE	
	IT SUPPORT	CERTIFICATE HELD	CERTIFICATE EXPIRY	10 STEPS ADOPTED?	

2 POLICY AND SCOPE

This business protects the systems and information it depends on — email, accounts and payroll, drawings and project documents, site records, CCTV — and the personal data it holds. The policy covers every device used for our work (office computers, laptops, phones and tablets on site, personal devices used for work email), every account, the office and site networks, and every person who uses them: directors, employees, agency workers and suppliers given access. The controls below follow the NCSC 10 Steps areas, scaled to the size of the business.

3 WHAT MATTERS MOST — CRITICAL SYSTEMS AND DATA

SYSTEM OR DATA	WHERE HELD — SUPPLIER	OWNER	BACKUP	RESTORE TESTED	MFA ON?

4 THE RULES

- 4.1 Accounts and access. Everyone has their own account — no shared log-ins. Multi-factor authentication is on for email, cloud services, banking, payroll and every administrator and remote access account. Passwords are long and not reused; a password manager is provided. Administrator rights go only to named people, who use a separate account for them. A leaver's access is removed on their last day; access is checked every six months.
- 4.2 Devices and updates. Only supported operating systems and software. Updates install automatically; any that cannot are applied within the deadline below — Cyber Essentials Requirements for IT Infrastructure v3.3 (April 2026) set 14 days from release for critical or high-risk updates. Default passwords on routers, CCTV recorders and site equipment are changed at installation. Screens lock when left. Software nobody uses is removed.
- 4.3 Firewalls and malware protection. A firewall on the office and site internet connections and on every laptop; malware protection on every computer; apps installed only from the official store or by IT support.
- 4.4 Phones and tablets on site. A PIN or biometric lock, encryption on, remote wipe set up. A lost or stolen device is reported to the responsible person the same day.
- 4.5 Backups. Critical systems in section 3 are backed up; at least one copy is kept separate from the network or in a service that cannot be altered from it, and enough history is kept to go back weeks, not days. Restores are tested at the interval below.
- 4.6 Email, phishing and payment fraud. Nobody opens an unexpected attachment or link, or enters a password from an email link. Any change of bank details, or an urgent request for payment, is confirmed by phone to a number already held. Suspicious emails are reported, not just deleted.
- 4.7 Home and site working. Work is done on business devices or on accounts protected by multi-factor authentication. Public Wi-Fi is not used without the business VPN — use the phone's hotspot instead. Devices are not left in vans or unlocked cabins. Printed drawings and records with personal data are shredded, not binned. The threats are assessed in 4.11.

CYBER SECURITY POLICY

continued

POLICY — COMPANY FILE

KD-PQ-CY-013 Rev A0

4.8 Logging and monitoring. Sign-in and security alerts are switched on for email and cloud services and go to a named person, who checks them; logs are kept for the period below so an incident can be traced.

4.9 Suppliers and subcontractors. IT and software suppliers have only the access they need, protected by multi-factor authentication, and removed when the work ends. Subcontractors given access to our systems or shared project platforms get their own accounts, limited to their package. Key subcontractors and suppliers handling our data are asked about their own cyber security before they start.

4.10 Training. Every new starter is briefed at induction; everyone gets a phishing and payment fraud briefing each year, recorded on KD-CAS-PB-005.

COMMITMENTS NOT ADOPTED — NUMBER AND REASON

CRITICAL UPDATES APPLIED WITHIN RESTORE TEST EVERY LOGS KEPT FOR ALERTS GO TO

4.11 Home and site working — threat assessment. Assess the threats to work done away from the office; revisit the table when the way people work changes.

THREAT	LIKELIHOOD H/M/L	CONTROL IN PLACE	OWNER
Laptop, phone or tablet lost or stolen from a van, cabin, car or home			
Shared or public Wi-Fi cafes, hotels, client or shared site networks			
Family or friends using a work device or work files on a personal device			
Screens and papers seen by others shoulder-surfing; drawings and records left out at home or in the cabin			
Phishing and fake calls aimed at people working away urgent payment or password requests, fake IT support			
Site router, CCTV recorder or smart kit on default settings default passwords, remote access left open			

ASSESSMENT DATE ASSESSED BY REVISIT BY

5 INCIDENT RESPONSE

An incident is anything that threatens the systems or data — a clicked phishing link, a device lost, ransomware, an account taken over, a payment sent to a fraudster. Anyone who suspects one tells the responsible person at once — at any hour; nobody is blamed for reporting. Then: 1 disconnect the affected device from the network, leave it on, and delete nothing; 2 call IT support; 3 change passwords from a clean device and end sessions; 4 for a payment, call the bank immediately; 5 decide with the data protection lead whether personal data is involved and must be reported (KD-PQ-DP-006 section 5); 6 tell the cyber insurer if there is one, before spending money on recovery; 7 restore from clean backups only after the cause is removed; 8 record what happened, what was done and what will change, and revise this plan.

INCIDENT LEAD — NAME, PHONE IT SUPPORT OUT OF HOURS BANK FRAUD LINE CYBER INSURANCE — POLICY, HELPLINE

PLAN LAST PRACTISED SCENARIO USED AND WHAT CHANGED

DATE	WHAT HAPPENED	AFFECTED	ACTION TAKEN	REPORTED TO	CLOSED

6 MICRO-BUSINESSES — THE SHORT STATEMENT ROUTE

Where the question set allows a micro-business to give a written statement instead of a policy (CAS v5 Q163), this box with sections 3 and 5 can stand for section 4 — check the size test your assessment body applies.

STATEMENT (MICRO-BUSINESS ONLY)

CYBER SECURITY POLICY

continued

POLICY — COMPANY FILE

KD-PQ-CY-013 Rev A0

7 RESPONSIBILITY, COMMUNICATION AND MONITORING

ROLE	NAME	WHAT THEY DO UNDER THIS POLICY

Evidence that the policy reached people: record each induction, briefing and issue on KD-CAS-PB-005 Policy Briefing and Acknowledgement Record — names, dates and signatures. Assessors ask for that record, dated within the last twelve months; only briefing people creates it.

HOW THE POLICY IS COMMUNICATED

HOW IT IS MONITORED, AND WHAT TRIGGERS AN EARLY REVISION

8 SIGNED FOR THE BUSINESS

I adopt this cyber security policy for the business named in section 1, and I will make sure it is resourced, briefed and kept current.

SIGNED — PRINTED NAME

POSITION

SIGNATURE

DATE

NEXT REVIEW DUE

R REVISION HISTORY

Every revision of this document, and every review that found nothing to change. The revision on the front of this sheet is the one you are holding — check kubitdocs.com for the current one before use.

Rev	Date	Class	What changed	Authorised by
D0	2026-09-13	first-issue	First issue.	— not yet approved —
A0	2026-09-13	review	Approved for issue by the author. Content unchanged from the reviewed draft; the draft status strip is removed. No independent third-party review has been carried out.	Author — director, UK principal contractor, SMSTS. Not an independent review.

Class: first-issue · material (the law, a control, a field or the scope changed — past buyers are notified) · editorial (wording or layout only) · review (checked, nothing changed) · withdrawal. Revision prefix D = draft, not approved and not for sale; A = approved for issue by the person named, on the date shown.