CLOUDSWITCHED

FREE RESOURCE — BACKUP RETENTION POLICY GUIDE

# Backup Retention Policy Guide

A written retention policy that you can sign, file and hand to an auditor or insurer. Set the tiered retention ladder, pin every data class to a legal or business obligation, evidence your compliance position, and lock in a quarterly review so the policy stays current as data, regulation and storage cost all change.

**4 tiers**
DAILY / WEEKLY MONTHLY / ARCHIVE

**7 years**
HMRC DEFAULT FINANCIAL RECORDS

**Quarterly**
POLICY REVIEW & SIGN-OFF

**Fillable**
TICK & TYPE IN ANY VIEWER

RETENTION LADDER | UK GDPR / DPA 2018 | HMRC | AUDIT-READY

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

# 00

# How to use this policy guide

A backup retention policy answers the two questions every regulator, auditor and cyber insurer will eventually ask: **how far back can you recover a given data class**, and **how long must you be able to produce it on request**. This guide turns those answers into a written, dated, signed policy — the artefact you produce when somebody outside the business asks "what is your retention policy?".

The five sections below build the policy in order. Read the prose, fill in the worksheets, then schedule the quarterly review. The value comes from the document being current and signed — not pristine.

> **RETENTION IS NOT THE SAME AS BACKUP FREQUENCY**
>
> A backup taken hourly with 24 hours of retention will let you recover the last day — not the last month. Retention is what you keep on the shelf; frequency is how often you write a new copy onto it. Pick both deliberately and write down the reason for each — that reason is what an auditor will read first.

## The five policy sections

- **01 Policy scope & legal framework** — what this policy covers, the obligations behind it, and the standard tier ladder.
- **02 Retention ladder & standard tiers** — the four-tier daily / weekly / monthly / archive default and your custom variations.
- **03 Retention schedule by data class** — one row per data class, pinned to a legal basis and retention period.
- **04 Compliance affirmations** — the checklist you tick to evidence the policy meets each obligation.
- **05 Policy ownership, version & review** — named owner, version, approval date, next review date and sign-off.

## Who needs to read and approve this policy

- **Policy Owner** — single accountable person; signs the policy and owns every retention decision.
- **Data Protection Lead / DPO** — confirms each retention period maps to a lawful basis and documented purpose.
- **Finance / Records Manager** — confirms HMRC, Companies Act and sector record-keeping rules are reflected.
- **Technical Owner** — confirms the backup product is configured to enforce the retention written here.

# 01

# Policy scope & legal framework

A retention policy that simply says “we keep backups” is worthless to an auditor. The policy has to name the **data classes** it applies to, the **legal or business basis** for each retention period, and the **storage and disposal rules** that the backup product is configured to enforce. This page sets that frame.

## Scope of this policy

This policy governs every backup copy of business data held by the organisation — on-premise, cloud, third-party SaaS backup copies, and any archival copies. It does **not** govern live production storage or retention inside source SaaS apps; those are covered by separate policies and referenced where they intersect with retention.

## Reference: typical UK SME obligations that drive retention

| OBLIGATION | TYPICAL PERIOD | WHAT IT COVERS |
|---|---|---|
| **UK GDPR / DPA 2018 storage limitation** | As short as practicable | Personal data — retention must be justified by a documented purpose; over-retention is itself a breach |
| **HMRC — business records** | 6 years + current | VAT, PAYE, corporation tax records, invoices, payroll, bank statements |
| **Companies Act 2006** | 6 years (some 10) | Accounting records, board minutes, register of members and PSCs |
| **Employment / pensions** | 6 years post-termination | Contracts, payslips, pension correspondence, leavers |
| **Cyber insurance & ISO 27001** | Per policy / Annex A.8.13 | Restore-test evidence, immutability of at least one tier, documented retention schedule |

## Principles this policy follows

- **Justified, not maximal** — each retention period is tied to a documented purpose; we do not keep data “just in case”.
- **Shortest defensible** — where two periods both satisfy obligations, the shorter wins, per UK GDPR storage limitation.
- **Tiered by frequency & age** — daily backups roll off into weekly, weekly into monthly, monthly into archive.
- **Immutable at the archive tier** — the longest-lived copy is held on write-once / Object Lock storage.
- **Encrypted at rest and in transit** — AES-256 at rest, TLS 1.2+ in transit, keys held separately with documented escrow.

# 02

# Retention ladder & standard tiers

The retention ladder is the cost-vs-recoverability trade-off, written down. A four-tier ladder — daily, weekly, monthly, archive — lets a recent backup roll off into successively longer-lived copies without paying to keep every nightly backup forever. Pick a default per tier, override per data class on the next page only when there is a documented reason.

### Reference: the standard four-tier ladder

| TIER | DEFAULT RETENTION | WHY THIS LENGTH |
|---|---|---|
| **Daily backups** | 30 days | Day-to-day recovery from accidental delete, file corruption, and the typical ransomware notice window |
| **Weekly backups** | 12 weeks | Recover from gradual corruption noticed weeks later |
| **Monthly backups** | 12 months | Year-on-year comparisons; recover the data set before a major change |
| **Annual / archive** | 7 years (or per law) | HMRC, Companies Act, employment records; cyber-insurance proof-of-record |

### Your retention ladder — defaults applied across the estate

Pick the default retention per tier. Any data class that needs a different number lives in Section 03; the entries here are the “unless otherwise stated” defaults.

| TIER | DEFAULT RETENTION | STORAGE LOCATION / MEDIA | NOTES / EXCEPTIONS |
|---|---|---|---|
| Daily backups | | | |
| Weekly backups | | | |
| Monthly backups | | | |
| Annual / archive | | | |

**IMMUTABILITY LIVES AT THE ARCHIVE TIER**

The longest-lived copy is the one a ransomware operator will try hardest to destroy. Whatever you choose — Object Lock on S3, hardened Veeam repository, tape with a real off-site rotation — it must be write-once for the retention period, with shortening credentials held in a separate identity scope.

# 03

# Retention schedule by data class

This is the operative table — one row per data class, pinned to a tier, a retention period and the legal or business basis that drives it. Every row gets a named business owner; the owner is the person who signs off the retention number and accepts the residual risk of choosing it. Add rows for every data class your organisation holds; the examples shown are starting points, not an exhaustive list.

### Retention schedule

| DATA CLASS | TIER | RETENTION | LEGAL / BUSINESS BASIS | IMMUTAB |
|---|---|---|---|---|
| Financial records (VAT, payroll, accounts) | | | | |
| Employee & HR records | | | | |
| Customer records / CRM data | | | | |
| Email / Microsoft 365 mailboxes | | | | |
| File shares (OneDrive, SharePoint, file server) | | | | |
| Teams chat & channel content | | | | |
| SQL / line-of-business database | | | | |
| Server images / VM backups | | | | |
| SaaS data (CRM / accounting / helpdesk) | | | | |
| Endpoint / laptop data | | | | |
| Network / firewall configs | | | | |
| Other — specify | | | | |

**PERSONAL DATA IS GOVERNED BY STORAGE LIMITATION**

Any row above that holds personal data (HR, customer records, mailboxes, CRM) is bound by the UK GDPR storage-limitation principle — you retain only as long as there is a documented purpose, then you delete. Pick the shortest defensible period for personal-data rows and capture the lawful basis in the “Legal / business basis” column so the policy itself is the evidence of compliance.

# 04

# Compliance affirmations

Each row below is a statement the Policy Owner attests to when this policy is signed. Tick each item only after the responsible owner has verified it — an unticked box is an open compliance gap to fix, accept as an exception, or schedule for remediation before next review.

### UK GDPR / Data Protection Act 2018

- ☐ **Storage limitation** — every retention period in Section 03 has a documented purpose; nothing is kept "just in case".
- ☐ **Lawful basis recorded** — each personal-data row references the lawful basis driving its retention (contract, legal obligation, legitimate interest).
- ☐ **Erasure handled** — documented approach for honouring erasure requests where retention obligations do not override.

### HMRC, Companies Act & sector record-keeping

- ☐ **HMRC 6-year minimum** — VAT, PAYE and corporation-tax records are retained for at least 6 years plus the current year.
- ☐ **Companies Act records** — accounting records, board minutes, registers of members and PSCs are retained for the statutory period.
- ☐ **Employment records** — contracts, payslips and pension correspondence retained for 6 years post-termination.
- ☐ **Sector regulator obligations** — where applicable (FCA, CQC, SRA), sector-specific retention is mapped and reflected.

### Security & cyber-insurance requirements

- ☐ **Encryption at rest** — AES-256 on every backup repository in scope of this policy.
- ☐ **Encryption in transit** — TLS 1.2 or higher between every backup agent and its repository.
- ☐ **Immutability at the archive tier** — the longest-lived copy is held on write-once / Object Lock / hardened-repository storage.
- ☐ **Restore tests evidenced** — documented restore-test evidence exists within the cadence required by our cyber-insurance policy.
- ☐ **Disposal logged** — data that has reached end-of-retention is purged on schedule and the deletion is recorded.

# 05

# Policy ownership, version & review

A retention policy without a named owner, a version and a date is a draft. This page assigns the owner, records the version, sets the next review date, and captures sign-off by the people whose attestations make the policy enforceable.

## Policy version & review

| FIELD | VALUE |
|---|---|
| Policy version | _____ |
| Effective date | _____ |
| Last reviewed | _____ |
| Next scheduled review | _____ |
| Document classification | _____ |

## Review cadence

- **Quarterly** — Policy Owner reviews the schedule against new data classes, retired systems and audit findings.
- **Annually** — full re-approval; all named signatories re-sign.
- **On material change** — new regulation, new data class or change of backup product / insurer triggers an out-of-cycle review.

## Approval & sign-off

| | | |
|---|---|---|
| POLICY OWNER | APPROVED BY | DATE |
| _____ | _____ | _____ |
| DATA PROTECTION LEAD | TECHNICAL OWNER | SENIOR SPONSOR |
| _____ | _____ | _____ |

# CLOUDSWITCHED

CLOUD BACKUP & DATA PROTECTION

**info@cloudswitched.com**

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