Data Retention Policy

Policy · US · Updated 2026-07-13 · Square brackets are placeholders to replace with your own details.

A data retention policy sets out how long your business keeps each type of record, why, and how records are securely destroyed when the time is up. It pairs a short set of rules with a retention schedule — the table your team actually uses — and a legal-hold mechanism that pauses destruction when a dispute or investigation is live.

Keeping everything forever feels safe but is the opposite: every record you hold is one more you have to protect, search when a request or lawsuit arrives, and account for if there is a breach. Old data is pure liability with no operational value — and in a breach, the difference between notifying last year's customers and notifying a decade of them is usually the retention policy you did or did not enforce.

This template gives you the policy rules, a retention schedule to complete by record type, secure disposal standards, and the legal-hold process, with the IRS's recordkeeping guidance as the anchor for the tax rows.

Purpose and scope

This policy sets out how long [Your company] retains business records and personal information and how they are disposed of. It applies to all records in all formats — databases, files, email, paper, backups, and archives — and to all staff who create or manage them.

Policy statement

[Your company] keeps records only as long as they are needed for a documented business, legal, or tax purpose, retains them for the periods in the schedule below, and disposes of them securely when the period ends. No one keeps personal copies, exports, or shadow spreadsheets outside the systems of record.

Responsibilities

- Policy owner ([name/role]): maintains this policy and the retention schedule, and declares and lifts legal holds.
- Record owners ([role per area, e.g. office manager for HR files, finance lead for accounts]): apply the schedule to their records and run periodic disposal.
- All staff: save records to the systems of record, not local drives or personal accounts, and flag records with no apparent owner or period.

How retention periods are set

- Legal, tax, or regulatory requirement: where a rule sets a period — tax records under current IRS recordkeeping guidance are the standard example — that period applies. Record the source; check current official guidance rather than folklore.
-

Potential claims: some records are kept for the period during which a legal claim could realistically arise — statutes of limitations vary by state and claim type, so take advice rather than guessing.

- Operational need: everything else is kept only as long as it is actually used, and the reason is written in the schedule.
- Where only statistics are needed long term, data is anonymized instead of retained.

Retention schedule

- Financial and tax records: [period — check current IRS recordkeeping guidance; the right period depends on the situation]. Reason/source: [complete].
- Payroll and employment records: [period — minimums are set by various federal and state rules; check current official guidance]. Reason/source: [complete].
- Hiring records, including applications from candidates not hired: [period]. Reason/source: [complete].
- Customer accounts and transaction records: [period] from the end of the relationship. Reason/source: [complete].
- Marketing lists and prospect data: [period] from last contact. Reason/source: [complete].
- Incident, accident, and insurance records: [period]. Reason/source: [complete].
- Security camera footage: [period — typically short] unless preserved for an incident. Reason/source: [complete].
- Email and general correspondence: [approach, e.g. deleted or archived after (period) unless filed as a record]. Reason/source: [complete].

Secure disposal

- Paper records are cross-cut shredded or placed in confidential waste via [provider] — never in the regular trash.
- Digital records are deleted from the system of record and any copies on shared drives; deletion is confirmed by the record owner.
- Devices being retired are securely wiped or destroyed via [certified provider], with certificates kept.
- Anything derived from consumer reports (background checks, credit information) is disposed of per current FTC disposal guidance.
- When a contract with a software or service provider ends, [name/role] confirms in writing that our data has been deleted or returned.
- Disposals of whole record classes are logged: what, when, by whom.

Legal holds

If litigation, a government investigation, an audit, or a complaint is live or reasonably expected, [name/role] declares a legal hold: routine destruction stops for all records in scope, and the affected record owners are told in writing. The hold overrides the schedule until [name/role] lifts it in writing. Destroying relevant records after a dispute has surfaced is far worse than keeping them too long — courts treat it that way too.

Records and review

The schedule, disposal logs, and hold notices are kept at [system/location]. This policy and the schedule are reviewed [frequency, e.g. annually] and whenever we adopt new systems, new record types, or new legal obligations — including new state privacy laws in the states where our customers live. Owner: [name/role]. Next review due: [date].

How to use this template

1. Inventory what you actually hold before touching the schedule — walk the shared drives, filing cabinets, and system exports first.
2. Complete the reason/source column for every row; a period with no justification is the first thing that fails scrutiny.
3. Check the tax rows against current IRS recordkeeping guidance, and the employment rows against current federal and state guidance — not memory.
4. Assign a named record owner to every row, then diary the first disposal run.
5. Do one supervised disposal run within a month of adopting the policy — the backlog is where the risk lives.
6. Cross-reference the schedule in your privacy policy so the two documents agree about how long customer data is kept.

Official guidance

- IRS — How long should I keep records?
- FTC — Protecting Personal Information: A Guide for Business
- FTC — Disposing of consumer report information