

Data Classification and Retention Policy

Owner	[Security owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	[Version]

1. Purpose and scope

This policy sets how [Company name] (the "Company") classifies the data it holds, how long it keeps each kind, and how it disposes of data it no longer needs. It supports the SOC 2 common criteria CC6.1 and CC6.5.

This policy applies to all company and customer data.

2. Classification levels

Every data set belongs to exactly one of the four levels below. When a data set mixes levels, it takes the highest level it contains. Unlabeled information is treated as Internal until it is classified.

Level	Definition	Examples
Restricted	Information whose disclosure would cause severe harm to customers or the Company, create legal or contractual liability, or enable an attacker to compromise systems.	Customer data stored in the Company's product; personal data of customers' users; authentication secrets, API keys, encryption keys and production credentials; payment card or bank details; employee government ID numbers and health information.
Confidential	Information intended for a defined group, whose disclosure would harm the Company, its customers or partners.	Source code; system architecture and network diagrams for the production cloud environment; security assessments, penetration test reports and vulnerability details; customer contracts and pricing; employee compensation and performance records; unreleased financials.
Internal	Information for use by personnel in the ordinary course of business, whose disclosure would cause limited harm.	Internal policies and procedures; team wikis and meeting notes; project plans and roadmaps without customer names; internal announcements; the org chart.

Level	Definition	Examples
Public	Information approved for release to anyone, whose disclosure causes no harm.	Marketing website content; published documentation for the Company's product; published blog posts and press releases; public job postings; the published privacy notice.

3. Handling rules

Personnel handle information according to the rules for its level. A rule for a lower level applies to every higher level unless a stricter rule replaces it.

Control	Restricted	Confidential	Internal	Public
Access	Named individuals with a documented business need, approved by the data owner and reviewed quarterly.	Role-based access for teams with a business need, reviewed at least every 6 months.	All personnel.	Anyone.
Storage	Only in approved production data stores or an approved secrets manager. Never on laptops, removable media, personal accounts or in source code.	Company-managed systems and Company accounts only. Not on personal devices or accounts.	Company-managed systems and Company accounts.	No restriction.
Sharing	Only with authorized recipients under a signed contract or data processing agreement, through an approved encrypted channel. Never by email attachment or chat.	Inside the Company on a need-to-know basis. Externally only under a signed non-disclosure agreement or contract.	Inside the Company. Externally only with manager approval.	Freely, once approved for release.
Retention	Kept only as long as the customer contract, law or documented business need requires, then deleted.	Kept for the period set in the retention schedule or contract.	Kept while useful to the business.	Kept while current.

Control	Restricted	Confidential	Internal	Public
Disposal	Deleted using provider deletion tools or cryptographic erasure; media wiped to National Institute of Standards and Technology (NIST) Special Publication 800-88 or physically destroyed; deletion recorded.	Secure deletion; devices wiped before reuse or disposal; paper shredded.	Standard deletion; paper shredded.	No restriction.

Restricted data is never used in development, testing or demo environments unless it has been irreversibly anonymized, and never pasted into public AI tools or unapproved third-party services.

Encryption requirements for each level are set in the Encryption Policy.

4. Retention schedule

Data is kept for the period below and then deleted or anonymized, unless a legal hold or a signed contract requires longer.

Record	Kept for	Owner
Customer data in production	The customer contract term, then deleted within [Deletion window]	[Engineering owner role]
Backups of customer data	[Backup retention period]	[Engineering owner role]
Security and audit logs	[Log retention period]	[Security owner role]
Audit evidence and policy records	[Evidence retention period]	[Security owner role]
Employee and contractor records	As required by employment law	[People owner role]

5. Disposal and deletion

- Retention: Data is retained according to contractual requirements and a defined retention schedule.
- Disposal: Data and media are disposed of using [Data destruction method].
- Customer deletion: When a contract ends or a customer asks for deletion, their data is deleted from production within [Deletion window] and from backups as those backups expire. Each deletion is recorded with its date.

- Devices: Laptops and storage media are wiped before reuse or disposal, and the wipe is recorded against the asset.

6. Roles and responsibilities

Role	Held by	Responsibility
Policy approver	[Policy approver role]	Approves this policy, each new version, and any risk the Company accepts instead of meeting it.
Policy owner	[Security owner role]	Maintains this policy, makes sure the controls in it operate, keeps the evidence, and reviews it at least once a year.
Data owner	[Security owner role]	Assigns each data set a level and approves access to Restricted and Confidential data.
All personnel	Everyone in scope	Follow this policy and report a suspected breach of it to the [Security owner role].

7. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

Record	What it shows	Where it is kept
Approved policy	This document, signed by the approver, with its version history.	[Documentation system]
Data classification scheme	Document defining data sensitivity levels.	[Documentation system]
Encryption configuration	Screenshots of database/storage encryption.	[Cloud provider]
Retention schedule	Document outlining data retention periods.	[Documentation system]
Deletion records	Customer data deletions and device wipes, with dates.	[Evidence storage location]

8. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

9. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

Version	Date	Summary of change	Approved by
[Version]	[Effective date]	First version.	[Policy approver role]

Policy approver

Name:

Signature:

Date:

10. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

Field	What to enter
[Company name]	Your legal company name.
[Effective date]	The date the approver signs this version.
[Version]	Start at 1.0 and increase it each time the document changes.
[Security owner role]	The role that runs the security program day to day, for example Chief Technology Officer.
[Policy approver role]	The officer who approves policies and accepted risks, for example Chief Executive Officer.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Documentation system]	Where policies and procedures are published, for example the company wiki.
[Cloud provider]	Where production runs, for example AWS, Google Cloud or Azure.
[Log retention period]	How long logs are kept, for example one year.
[Data destruction method]	How media and data are destroyed, for example to NIST SP 800-88.

Field	What to enter
[Backup retention period]	For example 30 days.
[Deletion window]	How soon customer data is deleted after a contract ends, for example 30 days.
[Evidence retention period]	How long audit evidence is kept, for example three years.
[People owner role]	The role that runs hiring and departures, for example head of people.
[Engineering owner role]	The role that owns production systems, for example engineering lead.
[Next review date]	The date this version must be reviewed by, at most 12 months after the effective date.

Source

Source: free template from www.polaralabs.com/templates/data-retention-policy (CC BY 4.0).