



EthicSuite™

powered by **Ethics Helpdesk (Pty) Ltd**

VERSION 2.2 · FINAL

Data Retention Policy

How long EthicSuite keeps information, and how it is securely disposed of

Document ID	ES-POL-004
Version	2.2
Status	Final
Classification	Internal
Policy owner	Information Officer
Approved by	Justin Veeran, Chief Executive Officer, on behalf of the Board of Directors of Ethics Helpdesk (Pty) Ltd
Policy period	28 February 2026 – 1 March 2027
Effective date	28 February 2026
Next review	1 March 2027

Approval

Signature	
Name	Justin Veeran
Title	Chief Executive Officer, Ethics Helpdesk (Pty) Ltd
Date	28 February 2026

Version history

Version	Date	Change
2.2	28 February 2026	Current issue, valid 28 February 2026 – 1 March 2027

1. Purpose

This policy sets out how long EthicSuite retains each category of information, how retention is applied, and how information is securely disposed of at the end of its retention period.

2. Scope

This policy applies to all information held by EthicSuite in any format, including production systems, backups, logs, email, support tools and third-party services.

3. Retention Principles

- Information is retained no longer than necessary for the purpose it was collected, subject to legal, regulatory and legitimate business requirements (POPIA section 14).
- Where EthicSuite acts as operator, the **tenant decides** the retention period for its case data within the platform limits; the defaults below apply when a tenant has not set its own period.
- Retention is automated wherever possible so that it does not rely on manual deletion.
- Information that is no longer needed in identifiable form, but is useful for statistics or reporting, is de-identified so it can no longer be linked to a person.

4. Retention Schedule

Retention periods start from the trigger event shown.

Data category	Default retention	Trigger	Basis / notes
Case data (reports, investigation notes, outcomes)	5 years (tenant-configurable 1–10 years)	Case closure	Tenant's legal and governance needs; Companies Act and Protected Disclosures Act
Reporter / vault data (identity-linking data)	Deleted or anonymised 90 days after case closure unless the reporter consents or a legal hold applies	Case closure	Data minimisation; protects reporter anonymity
Anonymous reporter messages	Same as case data	Case closure	Part of the case record
Recordings and evidence	Same as case data (5 years)	Case closure	Recordings that could identify a reporter by voice are held in the Restricted vault tier
Platform audit logs (case activity trail)	Life of the related case record, and at least 5 years	Log creation	Proves chain of custody and integrity of investigations
Security and system logs	12 months (90 days immediately searchable)	Log creation	ISO/IEC 27001; incident investigation
Backups	35 days rolling	Backup creation	Deleted data drops out when backups expire
Tenant data after contract end	Export available for 30 days; deleted within 90 days	Contract termination	Deletion certificate provided on request

Data category	Default retention	Trigger	Basis / notes
Financial and accounting records	7 years	End of financial year	Companies Act 71 of 2008 s24; Tax Administration Act 28 of 2011 (5 years minimum)
EthicSuite employee records	3 years after employment ends (5 years for tax records)	Termination	Basic Conditions of Employment Act s31; tax law
Support tickets	3 years	Ticket closure	Service quality and dispute resolution
Marketing and prospect data	Until consent is withdrawn or 24 months of inactivity	Last interaction	POPIA s69
Data subject and PAIA requests	5 years	Request closure	Evidence of compliance
Incident records	5 years	Incident closure	Evidence of compliance and lessons learned

5. Tenant-Configurable Retention

Tenant administrators can set retention periods for their case data within the platform limits. EthicSuite records every change to retention settings in the audit log, and warns administrators before settings would cause data to be deleted.

6. Secure Disposal

At the end of its retention period, information is disposed of using automated deletion from live systems, followed by cryptographic erasure (destroying the encryption keys) where data is encrypted per tenant or per record; deleted data is fully removed from backups when they expire. Physical media are destroyed in line with NIST SP 800-88, and cloud providers must certify their media destruction.

- Every disposal is logged (what, when, by which process), without keeping the deleted content.
- Tenants can request a certificate of deletion.
- Paper records are cross-cut shredded or destroyed by an approved provider.

7. Legal Hold

Information subject to a legal hold, investigation, litigation or regulatory requirement is retained beyond its normal retention period until the hold is lifted.

- Legal holds are issued by the Information Officer or legal counsel (or by the tenant, for its own data) and recorded in a legal hold register.
- Automated deletion is suspended for the data on hold.
- Holds are reviewed every 6 months and released as soon as they are no longer needed, after which normal retention resumes.

8. Roles and Responsibilities

Role	Responsibility
Information Officer	Owns this policy and the retention schedule; approves legal holds and changes.
Engineering lead	Implements and monitors automated retention and deletion jobs.
Data / system owners	Ensure their data is classified and mapped to the schedule.
Tenant administrators	Set retention for their own case data within platform limits.

9. Monitoring and Review

Automated deletion jobs are checked quarterly to confirm data is being deleted as scheduled. This policy is reviewed at least annually or following a change in law or in the data EthicSuite holds.