



TeamTrack

Data Retention & Secure Deletion Policy

Last updated and effective from: 8th June 2026

1 ABOUT THIS POLICY

1.1 THRIVE IT LTD. trading as TeamTrack ("we", "us" or "our") operates TeamTrack as a cloud-hosted Software-as-a-Service (SaaS) platform. This policy sets out the Company's approach to retaining, reviewing, securely deleting and disposing of personal data and business information processed during the operation of TeamTrack.

1.2 Objectives are to ensure personal data is retained only as long as necessary, comply with UK GDPR and contractual obligations, ensure secure deletion, minimise unnecessary retention, provide a consistent retention framework and support customer deletion instructions.

1.3 This policy applies to TeamTrack production systems, customer data, business records, backups, support systems, Company Directors, employees, contractors and approved third-party service providers.

1.4 This policy should be read alongside the Data Protection Policy, Privacy Policy, Freelancer Privacy Policy, Information Security Policy, Business Continuity & Disaster Recovery Policy, Data Processing Agreement, Data Breach Policy and Terms of Service.

2 RETENTION PRINCIPLES

- Personal data shall be retained only for as long as necessary for the purpose for which it was collected.
- Retention periods are determined by legal, contractual, operational, security and business continuity requirements.
- Where TeamTrack acts as data processor, the Customer determines operational retention periods subject to applicable law.
- Information no longer required shall be securely deleted, anonymised or returned where appropriate.

3 RETENTION FRAMEWORK

3.1 The Company maintains the Retention Schedule contained in Appendix A. Retention periods may be amended where legal, regulatory or operational requirements change.

4 CUSTOMER DATA

4.1 Customer data remains under the control of the Customer. Following termination, customer data shall be exported, returned, deleted or anonymised in accordance with the Data Processing Agreement, customer instructions and applicable law.

5 BACKUPS

5.1 Production backups are maintained solely for disaster recovery and business continuity.

5.2 Production backups are retained for 60 days.

5.3 Deleted customer records remain deleted from production immediately but may continue to exist within production backups until the applicable backup retention period expires.

5.4 Expired backup data is securely removed through normal backup lifecycle management.

6 SECURE DELETION

6.1 Secure deletion methods include secure deletion from databases and cloud storage, cryptographic erasure where supported, destruction of physical media, automated cloud lifecycle deletion and anonymisation where appropriate.

7 CUSTOMER OFFBOARDING

7.1 Customers may request export or return of their data before deletion. Following completion of any agreed export process, production data shall be securely deleted. Residual copies within backups expire automatically after the 60-day backup retention period.

8 LEGAL HOLDS

8.1 Normal deletion may be suspended where information is subject to litigation, regulatory investigation, law enforcement requests or other legal preservation obligations.

9 RESPONSIBILITIES

9.1 Company Directors are responsible for approving retention periods, exceptions and policy reviews.

9.2 Personnel shall comply with retention requirements and securely dispose of information when instructed.

10 REVIEW

10.1 Retention periods and deletion processes shall be reviewed periodically and at least annually.

11 RELATED POLICIES

11.1 This policy should be read alongside the following Company policies and contractual documents:

- TeamTrack Information Security Policy
- TeamTrack Data Protection Policy
- TeamTrack Data Breach Policy
- TeamTrack Acceptable Use Policy
- TeamTrack Privacy Policy
- TeamTrack Data Processing Agreement
- TeamTrack Terms of Service
- TeamTrack Third Party Sub-Processor Register

Together these documents provide the Company's governance framework for information security, business continuity, data protection and the secure operation of the TeamTrack Service.

12 QUESTIONS ABOUT THIS POLICY

Questions regarding this policy should be referred to the Company Directors at:

support@teamtrack.uk

13 KEEPING THIS POLICY UP TO DATE

13.1 This policy shall be reviewed:

- at least annually
- following a significant disaster recovery event
- following material changes to the TeamTrack platform or cloud infrastructure
- following significant changes to the Company's operational processes
- where changes in legislation, regulation or recognised good practice make review appropriate

13.2 The Company Directors are responsible for ensuring this policy remains appropriate to the Company's operations and reflects the current TeamTrack production environment.

13.3 Material amendments shall be communicated to all relevant personnel.

Appendix A – Retention Schedule

Information Category	Standard Retention Period
Customer production data	Duration of customer contract or customer instruction
Deleted customer records	30 days following deletion from production plus the 60-day production backup retention period
Production backups	60 days
Customer support tickets	Up to 7 years
Customer billing records	Up to 7 years
Contracts and legal records	Up to 7 years after termination
Company accounting records	As required by law
Security logs	Normally up to 12 months
Audit logs	Normally up to 12 months
Penetration testing reports	Up to 7 years
Internal security documentation	Until superseded or no longer required

Appendix B – Data Disposal Decision Flow

Is the information still required?

Yes → Retain

No → **Legal or contractual obligation?**

Yes → Retain until obligation expires

No → **Customer requested export?**

Yes → Export then securely delete

No → Securely delete

Residual copies in backups expire automatically after the 60-day backup retention period.