



TeamTrack

Business Continuity & Disaster Recovery Policy

Last updated and effective from: 25th May 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 maintaining business continuity and restoring the availability of the TeamTrack platform following a significant operational disruption or disaster.

1.2 The objectives of this policy are to:

- a) minimise disruption to customers
- b) restore critical services as quickly and safely as reasonably practicable
- c) minimise the loss of customer data
- d) provide a structured approach to disaster recovery
- e) ensure recovery activities are coordinated and appropriately documented
- f) support continual improvement of the Company’s resilience and recovery capabilities

1.3 This policy applies to:

- the TeamTrack production platform
- Google Cloud Platform infrastructure supporting the Service
- supporting operational cloud services required for delivery of the Service
- Company Directors
- the Chief Technical Officer (CTO)
- any third-party suppliers engaged to assist with disaster recovery

1.4 This policy applies to significant operational incidents affecting the availability, integrity or recoverability of the TeamTrack platform, including but not limited to:

- loss of production services
- failure of critical Google Cloud infrastructure
- corruption or loss of production data
- significant cyber security incidents
- software deployment failures affecting service availability
- prolonged outages affecting critical third-party services
- other incidents that materially affect the Company’s ability to provide the Service

1.5 This policy forms part of the Company’s wider Information Security and Business Governance framework and should be read alongside:

- TeamTrack Information Security Policy
- TeamTrack Data Protection Policy
- TeamTrack Data Breach Policy
- TeamTrack Acceptable Use Policy
- TeamTrack Data Processing Agreement

- TeamTrack Terms of Service
- TeamTrack Third Party Sub-Processor Register

Those documents contain detailed requirements relating to information security, data protection, incident response, supplier management and customer obligations. This policy focuses specifically on maintaining service continuity and recovering the TeamTrack platform following a disaster and does not repeat those requirements.

2 BUSINESS CONTINUITY OBJECTIVES

2.1 The Company aims to maintain the availability and resilience of the TeamTrack platform through the use of professionally managed cloud infrastructure, resilient system design, regular backups and documented recovery procedures.

2.2 Where a disaster occurs, recovery activities shall seek to:

- restore customer access to the TeamTrack platform as quickly as reasonably practicable
- minimise disruption to customers
- protect the confidentiality, integrity and availability of customer information
- maintain clear communication with affected customers
- restore normal business operations in a controlled manner

2.3 Recovery priorities shall be determined by the Company Directors in consultation with the Chief Technical Officer (CTO), taking account of:

- customer impact
- operational priorities
- information security considerations
- regulatory obligations
- technical feasibility

2.4 The Company shall maintain documented recovery procedures appropriate to the TeamTrack platform and supporting cloud infrastructure.

These procedures shall be reviewed periodically and updated following significant changes to the platform or lessons learned from operational incidents.

3 RECOVERY TARGETS

3.1 The Company maintains recovery objectives to support business continuity planning.

These objectives are reviewed periodically and may be amended as the TeamTrack platform evolves.

Recovery Time Objective (RTO)

The target maximum period within which the TeamTrack production service should be restored following a declared disaster is:

Four (4) hours

Recovery Point Objective (RPO)

The target maximum acceptable loss of production data following a declared disaster is:

Fifteen (15) minutes

3.2 These objectives represent operational targets rather than contractual service level commitments.

Actual recovery times will depend upon:

- the nature of the incident
- the availability of third-party services
- the extent of any infrastructure failure
- the effectiveness of recovery procedures

4 DECLARING A DISASTER

4.1 Not every service interruption requires activation of this policy.

This policy shall be activated only where an incident is likely to have a significant impact on the availability, integrity or recoverability of the TeamTrack platform, or where normal operational procedures are unlikely to restore service within an acceptable timeframe.

4.2 Examples of incidents that may require activation of this policy include:

- prolonged outage of the TeamTrack production platform
- significant failure of Google Cloud services supporting production
- corruption or loss of production databases
- unsuccessful software deployment resulting in major service disruption
- cyber security incidents significantly affecting service availability
- failure of critical third-party cloud services
- any other incident considered by the Company Directors to require formal disaster recovery

4.3 The decision to declare a disaster rests with the Company Directors following consultation with the Chief Technical Officer (CTO), where reasonably practicable.

Once declared, recovery activities shall be coordinated in accordance with this policy.

5 ROLES AND RESPONSIBILITIES

5.1 The Company Directors are responsible for the overall management of disaster recovery activities.

Their responsibilities include:

- declaring a disaster where appropriate
- determining business priorities during recovery
- coordinating recovery with the Chief Technical Officer (CTO)
- communicating with customers where necessary
- liaising with third-party suppliers
- approving the return to normal service

5.2 The Chief Technical Officer (CTO) is responsible for coordinating the technical recovery of the TeamTrack platform.

Responsibilities include:

- assessing the technical impact of the incident
- identifying affected systems and services
- coordinating restoration of production services
- validating the integrity and availability of restored systems
- recommending improvements following recovery

5.3 Where specialist assistance is required, the Company Directors may engage approved suppliers, including authorised service providers, to assist with recovery activities.

6 RECOVERY STRATEGY

6.1 TeamTrack has been designed as a cloud-native Software-as-a-Service platform using professionally managed cloud infrastructure.

The Company's recovery strategy is based upon:

- resilient cloud infrastructure
- managed cloud services
- documented recovery procedures
- regular backups
- controlled deployment processes
- secure restoration of production services

6.2 The Company seeks to recover services using existing cloud infrastructure wherever reasonably practicable before considering more extensive recovery measures.

6.3 Recovery activities may include:

- restoration of production services
- rollback of software deployments
- recovery of databases from backups
- restoration of cloud configuration
- recovery of integrated services
- validation of production data

6.4 Detailed technical implementation procedures, deployment processes and operational runbooks are maintained separately from this policy to ensure they remain current as the TeamTrack platform evolves.

7 BACKUPS AND DATA RECOVERY

7.1 The Company maintains backup arrangements appropriate to the TeamTrack production environment.

Backups are intended to support recovery following accidental data loss, infrastructure failure or other significant operational incidents.

7.2 The Company shall periodically review backup arrangements to ensure they continue to meet business recovery objectives.

Where appropriate, restoration testing shall be undertaken to verify the effectiveness of backup procedures.

7.3 The detailed management of customer information, retention periods and deletion requirements is governed by the TeamTrack Data Protection Policy and Data Processing Agreement and is not repeated within this policy.

7.4 Where customer data must be restored following a disaster, restoration shall be undertaken using approved recovery procedures designed to preserve the confidentiality, integrity and availability of customer information.

8 RECOVERY PROCESS

8.1 Following declaration of a disaster, recovery activities shall normally follow the stages below:

Stage 1 – Assessment

The Company shall:

- identify affected services
- assess business impact
- determine recovery priorities
- identify immediate actions required

Stage 2 – Containment

Where appropriate, steps shall be taken to prevent further service degradation, data loss or security risk before recovery begins.

Stage 3 – Recovery

Recovery activities may include:

- restoring production services
- restoring cloud infrastructure
- recovering production databases
- validating application functionality
- confirming successful authentication and access

Stage 4 – Validation

Before normal operations resume, the Company shall verify that:

- critical services are operational
- production data is intact
- customer access has been restored
- monitoring confirms normal system operation

Stage 5 – Return to Service

The Company Directors shall authorise the return to normal operational status once they are satisfied that recovery objectives have been achieved.

9 COMMUNICATIONS DURING A DISASTER

9.1 The Company recognises the importance of providing timely and accurate information during significant service disruptions.

9.2 The Company Directors are responsible for customer communications throughout a disaster recovery event.

9.3 Communications may be provided using:

- LiveAgent (TeamTrack Support Emails)
- email
- the TeamTrack website
- other appropriate communication channels

9.4 Customer communications should, where appropriate, include:

- a description of the affected services
- the known customer impact
- recovery progress where available
- confirmation when services have been restored

The Company will seek to provide accurate information while recognising that technical details may evolve as an incident is investigated.

10 TESTING AND CONTINUAL IMPROVEMENT

10.1 The Company shall periodically test its Business Continuity and Disaster Recovery arrangements to provide assurance that recovery procedures remain effective and appropriate for the TeamTrack platform.

10.2 Testing may include:

- restoration of production backups;
- recovery of cloud infrastructure;
- validation of recovery procedures;

- verification of critical third-party service availability;
- review of operational documentation.

Testing shall reflect the Company's current production environment and operational practices.

10.3 The Company aims to perform disaster recovery testing at least annually and following significant changes to the TeamTrack platform or supporting cloud infrastructure where appropriate.

10.4 Following each recovery exercise or significant operational incident, the Company shall review:

- recovery objectives
- effectiveness of recovery procedures
- recovery times achieved
- lessons learned
- opportunities for improvement

Where improvements are identified, this policy and any supporting operational documentation shall be updated accordingly.

11 CONTINUAL SECURITY ASSURANCE

11.1 Business Continuity and Disaster Recovery form part of the Company's wider Information Security Management framework.

The Company maintains a programme of continual security assurance to improve the resilience of the TeamTrack platform.

11.2 This programme includes, where appropriate:

- annual independent penetration testing
- periodic review of user access permissions
- vulnerability management
- security updates
- backup verification
- disaster recovery testing
- review of third-party suppliers
- annual policy reviews

Detailed requirements relating to information security are contained within the TeamTrack Information Security Policy.

12 THIRD-PARTY SERVICES

12.1 The availability of TeamTrack depends upon several approved cloud service providers.

The Company maintains awareness of these dependencies when assessing business continuity risks and recovery priorities.

12.2 Where a disaster involves the failure of a third-party supplier, the Company shall:

- assess the impact upon TeamTrack
- engage with the supplier where appropriate
- implement reasonable mitigation measures
- keep affected customers informed where necessary

12.3 Detailed information relating to approved suppliers, sub-processors and data processing arrangements is maintained separately within the:

- TeamTrack Third Party Sub-Processor Register
- TeamTrack Data Processing Agreement
- TeamTrack Information Security Policy

Those documents should be referred to where additional supplier information is required.

13 RELATED POLICIES

13.1 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.

14 QUESTIONS ABOUT THIS POLICY

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

support@teamtrack.uk

15 KEEPING THIS POLICY UP TO DATE

15.1 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

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

15.3 Material amendments shall be communicated to all relevant personnel.