Information Technology & Information Security 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") develops and operates the TeamTrack Software-as-a-Service (SaaS) platform. Information security is fundamental to the operation of our business and to maintaining the trust of our customers.

This policy defines the Company's approach to protecting its information systems, cloud infrastructure and technology assets from unauthorised access, misuse, loss, disruption and cyber security threats.

1.2 TeamTrack operates a cloud-first technology environment. Our production platform is hosted entirely within Google Cloud Platform (GCP), and our internal business operations are supported primarily by cloud-based Software-as-a-Service providers.

The Company does not operate on-premise production servers, traditional corporate network infrastructure or internal datacentres.

1.3 This policy sets out:

a) the principles governing information security within TeamTrack;
b) how access to Company systems is managed;
c) how TeamTrack secures its cloud infrastructure;
d) the Company's approach to secure software development;
e) how technical vulnerabilities are identified and managed;
f) how the Company demonstrates ongoing security assurance.

1.4 This policy applies to:

- company directors
- employees
- contractors
- consultants
- temporary workers
- any third party granted authorised access to Company systems

All personnel are required to comply with this policy.

1.5 This policy applies to all Company technology resources including:

- the TeamTrack SaaS platform
- Google Cloud Platform infrastructure
- Jira
- LiveAgent
- GoCardless
- QuickBooks
- Microsoft 365
- source code repositories

- Company-issued computing devices
- any other approved cloud service used to support Company operations

1.6 This policy forms part of the Company's wider Information Security and Data Protection framework and should be read alongside:

- 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
- TeamTrack Business Continuity & Disaster Recovery

Those documents contain the Company's detailed requirements relating to data protection, acceptable use, breach management, privacy obligations, customer contractual obligations, and third-party processing. This policy intentionally avoids repeating those requirements and instead focuses on the security governance of TeamTrack's technology environment.

2 INFORMATION SECURITY PRINCIPLES

2.1 The Company designs, develops and operates TeamTrack in accordance with recognised information security principles.

Information security shall be considered throughout the lifecycle of all Company systems, software and cloud infrastructure.

2.2 The Company seeks to ensure the:

- **Confidentiality** - Information is accessible only by authorised individuals.
- **Integrity** - Information remains accurate, complete and protected against unauthorised modification.
- **Availability** - Systems remain available and resilient to support the delivery of TeamTrack services.
- **Least Privilege** - Users are granted only the minimum access necessary to perform their duties.
- **Defence in Depth** - Multiple complementary technical and organisational security controls are implemented to reduce overall security risk.

2.3 Security is and shall be incorporated into:

- system design
- software development
- deployment
- operational management
- supplier selection
- ongoing maintenance

2.4 All users share responsibility for protecting Company systems and customer information by complying with this policy and the Company's related security policies.

3 CLOUD INFRASTRUCTURE

3.1 TeamTrack operates entirely as a cloud-hosted Software-as-a-Service platform.

Production systems are hosted within Google Cloud Platform using services including Google Compute Engine, Google App Engine and other managed Google Cloud services appropriate to the operation of the platform.

3.2 The Company adopts managed cloud services wherever practical to improve:

- resilience
- scalability
- operational security
- service availability
- disaster recovery capabilities

3.3 Administrative access to production cloud infrastructure shall:

- be restricted to authorised personnel
- use named user accounts
- require Multi-Factor Authentication
- be granted according to business need
- be reviewed periodically

3.4 Changes to production infrastructure shall follow controlled operational processes and be appropriately documented.

Unauthorised changes to production systems are prohibited.

3.5 Customer operational data should remain within the TeamTrack platform wherever reasonably practical.

Limited customer information may be processed within approved business systems such as LiveAgent, QuickBooks, Jira or Microsoft 365 where necessary to support legitimate business operations.

Detailed requirements relating to the processing, sharing and protection of personal data are contained within the TeamTrack Data Protection Policy and Data Processing Agreement.

4 IDENTITY AND ACCESS MANAGEMENT

4.1 The Company controls access to its systems and information through Identity and Access Management (IAM) principles.

Access shall only be granted where it is necessary for an individual to perform their authorised duties.

4.2 The Company applies the Principle of Least Privilege when assigning permissions to all Company technology resources listed in section 1.5.

Users shall receive only the permissions necessary for their role.

4.3 All users shall be allocated an individual user account.

Shared user accounts shall not be used except where technically unavoidable for system-to-system integrations or service accounts. Such accounts shall be appropriately secured, documented and reviewed.

4.4 Multi-Factor Authentication (MFA) shall be enabled for all administrative accounts and wherever supported by Company systems.

Administrative access to production systems shall not rely solely upon passwords.

4.5 Passwords shall be:

- unique to each system
- kept confidential
- appropriately complex
- stored securely

The Company encourages the use of an approved password manager for generating and maintaining unique credentials.

4.6 User access shall be reviewed:

- when individuals join the Company
- when responsibilities change
- when individuals leave the Company
- periodically as part of routine security reviews

Access that is no longer required shall be removed promptly.

5 SECURE SOFTWARE DEVELOPMENT

5.1 The security of TeamTrack depends upon secure software development throughout the Software Development Lifecycle (SDLC).

Security shall be considered during:

- solution design
- software development
- testing
- deployment
- maintenance

5.2 Software development activities shall be managed using Jira to provide an auditable record of development work, software defects, enhancements and production changes.

5.3 Source code shall be maintained within approved version control repositories.

The Company shall maintain version history sufficient to support:

- change tracking
- peer review
- rollback where appropriate
- audit requirements

5.4 Changes to production software should be subject to appropriate review and testing before deployment.

Where practical this should include:

- peer review
- functional testing
- regression testing
- security review where appropriate

Emergency security fixes may follow an expedited process where required to protect the security or availability of the Service.

5.5 Developers shall follow secure coding practices designed to reduce common software vulnerabilities, including:

- injection attacks
- broken access control
- insecure authentication
- cross-site scripting
- insecure file handling
- insecure API implementations

5.6 Sensitive information including passwords, API keys, encryption keys and authentication tokens shall not be stored within source code repositories.

Secrets shall be managed using Google Secret Manager.

5.7 Third-party software libraries and dependencies shall be reviewed periodically and updated where appropriate to address known security vulnerabilities.

Detailed requirements relating to the this can be found in the TeamTrack UK Secure Software Development Policy.

6 APPROVED CLOUD SERVICES

6.1 The Company operates primarily through approved cloud-based Software-as-a-Service providers.

Only services approved by the Company Directors may be used to process Company or customer information.

6.2 Current approved operational platforms include:

Service	Primary Purpose
Google Cloud Platform	Production hosting and infrastructure
Microsoft 365	Email, collaboration and document creation
LiveAgent	Customer support
Jira	Software development and issue management
GoCardless	Payment processing
QuickBooks	Accounting and financial management
Zoom	Video calls with colleagues and customers
Microsoft Teams	Video calls with customers
Slack	Internal communications

The approved supplier list may be amended from time to time as operational requirements evolve.

6.3 Before introducing a new cloud service, the Company shall consider:

- business need
- security controls
- contractual arrangements
- data protection obligations
- supplier reliability
- operational risk

Approval of the Company Directors shall be obtained before Company or customer information is processed using any new service.

6.4 Detailed information regarding approved sub-processors, international transfers and data processing arrangements is maintained separately within the:

- TeamTrack Third Party Sub-Processor Register
- TeamTrack Data Processing Agreement
- TeamTrack Privacy Policy

Those documents should be referred to where additional detail is required.

7 CUSTOMER INFORMATION

7.1 The TeamTrack platform is the primary location for customer operational data.

The Company seeks to minimise duplication of customer information across multiple systems.

7.2 Where customer information is processed outside TeamTrack for legitimate business purposes, only approved Company systems shall be used. Examples include:

- customer support
- billing
- software issue investigation
- reporting
- customer communications

7.3 Customer information shall not be copied into:

- personal email accounts
- personal cloud storage
- unauthorised Software-as-a-Service platforms

- consumer messaging services

7.4 Detailed requirements governing:

- lawful processing
- information sharing
- retention
- deletion
- data subject rights
- international transfers
- processor obligations

are contained within the TeamTrack Data Protection Policy, Privacy Policy and Data Processing Agreement and are not repeated within this policy.

8 VULNERABILITY MANAGEMENT AND SECURITY ASSURANCE

8.1 The Company is committed to identifying, assessing and remediating security vulnerabilities throughout the TeamTrack platform and supporting cloud infrastructure.

Vulnerability management is an ongoing process designed to reduce the likelihood and impact of cyber security threats.

8.2 The Company shall maintain appropriate processes for:

- monitoring published security advisories
- reviewing software dependencies
- applying security updates
- assessing newly identified vulnerabilities
- implementing security improvements where appropriate

Critical vulnerabilities affecting production systems shall be assessed and remediated as soon as reasonably practicable.

8.3 The Company shall commission an independent penetration test of the TeamTrack production platform and associated cloud infrastructure at least annually.

Additional penetration testing may be undertaken following significant architectural changes or where the Company considers it appropriate to do so.

8.4 Penetration testing shall be performed by suitably qualified independent security professionals.

The scope of testing should include, where appropriate:

- externally accessible services
- web application security
- authentication mechanisms
- authorisation controls
- APIs
- cloud infrastructure
- common application security vulnerabilities

8.5 Penetration testing findings shall be:

- reviewed by the Company Directors
- prioritised according to business risk
- tracked through to completion
- used to improve the overall security posture of TeamTrack

Evidence of penetration testing and remediation shall be retained as part of the Company's compliance records.

9 LOGGING, MONITORING AND SECURITY REVIEW

9.1 The Company maintains appropriate logging and monitoring to support:

- operational management
- security monitoring
- incident investigation
- audit requirements
- service reliability

9.2 Where appropriate, logging may include:

- user authentication events
- administrative activity
- production deployments
- application errors
- infrastructure events
- security alerts

Access to security logs shall be restricted to authorised personnel.

9.3 The Company shall periodically review security events and operational alerts to identify:

- unauthorised access attempts
- unusual account activity
- operational issues
- opportunities to improve security controls

9.4 Monitoring is undertaken solely for legitimate business purposes including:

- protecting Company systems
- maintaining service availability
- investigating incidents
- meeting contractual and regulatory obligations

10 BUSINESS CONTINUITY

10.1 The Company recognises that service availability is essential to customers using TeamTrack.

Business Continuity arrangements are intended to minimise disruption following technical failures, cyber security incidents or significant operational events.

10.2 The Company's cloud-first architecture provides resilience through professionally managed infrastructure within Google Cloud Platform.

Where reasonably practicable, the Company seeks to minimise single points of failure within production systems.

10.3 The Company shall maintain appropriate arrangements for:

- production backups
- recovery of critical systems
- restoration of services following major incidents
- review of disaster recovery procedures

10.4 Backup and recovery procedures shall be reviewed periodically.

Where appropriate, recovery testing shall be undertaken to confirm that backup arrangements remain effective.

10.5 Business Continuity arrangements shall be reviewed following:

- significant infrastructure changes
- major service incidents
- material changes to operational processes

Detailed requirements relating to the this can be found in the TeamTrack Business Continuity & Disaster Recovery Policy.

11 INFORMATION SECURITY INCIDENTS

11.1 All personnel are responsible for promptly reporting suspected information security incidents, including:

- suspected unauthorised access
- compromised credentials
- phishing attacks
- malware
- security alerts
- attempted cyber attacks
- unexpected service disruption

11.2 All suspected incidents shall be reported immediately to the Company Directors.

11.3 Information security incidents shall be investigated, documented and reviewed to identify:

- root cause
- impact
- corrective actions
- opportunities for continual improvement

11.4 Where an incident involves personal data, staff shall follow the TeamTrack Data Breach Policy.

The identification, investigation, reporting and management of personal data breaches are governed entirely by that policy and are not repeated within this document.

12 STAFF RESPONSIBILITIES

12.1 Every individual with access to Company systems contributes to the security of TeamTrack.

Users shall:

- comply with this policy
- protect Company accounts and credentials
- use only approved systems
- maintain Multi-Factor Authentication where available
- report suspected security incidents promptly
- participate in security awareness training where required

12.2 Detailed requirements relating to:

- acceptable use
- password management
- handling personal data
- reporting data breaches
- user responsibilities

are contained within the TeamTrack Acceptable Use Policy, Data Protection Policy and Data Breach Policy.

13 RELATED POLICIES

13.1 This policy should be read alongside the following TeamTrack policies and contractual documents:

- Data Protection Policy
- Data Breach Policy
- Acceptable Use Policy
- Privacy Policy

- Data Processing Agreement
- Terms of Service
- Third Party Sub-Processor Register

Each document addresses a specific area of governance and together forms the Company's Information Security and Data Protection framework.

14 QUESTIONS ABOUT THIS POLICY

Questions regarding this policy should be directed 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 significant changes to the TeamTrack platform or cloud infrastructure;
- following significant security incidents;
- following changes to applicable legislation or recognised security best practice.

15.2 The Company Directors are responsible for approving and maintaining this policy.

15.3 Material changes shall be communicated to all relevant personnel.