Secure Software Development Policy

Last updated and effective from: 30 June 2026

1 ABOUT THIS POLICY

1.1 THRIVE IT LTD. trading as TeamTrack operates TeamTrack as a cloud-hosted Software-as-a-Service (SaaS) platform. This policy sets out the Company's requirements for the secure design, development, testing, deployment and maintenance of TeamTrack software.

1.2 The objectives of this policy are to embed security throughout the software development lifecycle, protect customer and Company information, reduce vulnerabilities before software reaches production, support compliance with UK GDPR and recognised security standards, and promote continual improvement of secure development practices.

1.3 This policy applies to all software developed by or on behalf of the Company, including web applications, mobile applications, APIs, internal tools and supporting services. It applies to all employees, contractors and third-party developers involved in software development.

1.4 This policy forms part of the Company's wider Information Security Management framework and should be read alongside the Information Security Policy, Data Protection Policy, Data Breach Policy, Acceptable Use Policy, Privacy Policy, Data Processing Agreement, Terms of Service and Third-Party Sub-Processor Register.

2 SECURE DEVELOPMENT OBJECTIVES

2.1 The Company adopts a security-by-design approach.

2.2 Security considerations shall be incorporated from project initiation through design, development, testing, deployment and maintenance.

2.3 The Company applies the principles of Security by Design and Default, Least Privilege, Defence in Depth, Zero Trust, Privacy by Design and Shift Left Security, ensuring security activities begin early within the development lifecycle rather than after software has been completed.

3 SECURE DEVELOPMENT GOVERNANCE

3.1 The Company shall define security requirements during project planning, undertake threat modelling for significant new functionality, identify sensitive data flows, attack surfaces and regulatory obligations, and ensure appropriate security controls are incorporated into solution designs.

4 SECURE DEVELOPMENT LIFECYCLE

4.1 Planning and Requirements: Security requirements shall be established during project initiation and reviewed throughout delivery.

4.2 Design: Secure architecture patterns shall be used to reduce exposure to common vulnerabilities, including the OWASP Top 10. Designs shall consider encryption, authentication, authorisation and secure API design.

4.3 Development: Developers shall follow secure coding standards, validate inputs, sanitise outputs, avoid hard-coded credentials and use only approved libraries and frameworks.

4.4 Testing: Security testing includes Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), software composition/dependency scanning and manual code review.

4.5 Deployment: Deployments shall utilise secure CI/CD pipelines, access controls, automated security checks, secure vault-based secrets management and Infrastructure as Code (IaC) security practices.

4.6 Maintenance: Applications shall be monitored for vulnerabilities, patched regularly and subjected to ongoing penetration testing where appropriate.

5 APPLICATION SECURITY REQUIREMENTS

5.1 Web applications shall protect against recognised application security risks including the OWASP Top 10. HTTPS (TLS 1.2 or later), secure session management, rate limiting, input validation and output encoding shall be implemented where appropriate.

5.2 Mobile applications shall minimise local storage of sensitive information, use platform-provided secure storage, enforce secure API communication and, where reasonably practicable, implement measures to reduce the risk of reverse engineering and execution on compromised devices.

6 IDENTITY, AUTHENTICATION AND ACCESS CONTROL

6.1 APIs shall require appropriate authentication and authorisation, validate inputs and implement logging and rate limiting.

6.2 The Company shall implement Multi-Factor Authentication (MFA) where appropriate, support recognised authentication standards such as OAuth2 or OpenID Connect, enforce strong password policies and apply Role-Based Access Control (RBAC).

7 DATA PROTECTION AND PRIVACY BY DESIGN

7.1 Software shall support the principles of Privacy by Design. Personal data shall be minimised, encrypted in transit and at rest, and processed in accordance with UK GDPR including lawful processing and support for data subject rights.

8 THIRD-PARTY COMPONENTS, SECRETS AND SUPPLY CHAIN SECURITY

8.1 Only approved third-party libraries and frameworks may be used. Dependencies shall be monitored for known vulnerabilities (CVEs), updated regularly and subject to software composition analysis where appropriate.

8.2 Secrets shall never be stored in source code or exposed in logs and shall instead be managed using approved secure secret management solutions with periodic rotation.

9 LOGGING, MONITORING AND VULNERABILITY MANAGEMENT

9.1 Applications shall generate appropriate security logs including authentication events, errors, exceptions and security-related activity whilst avoiding unnecessary exposure of sensitive information.

9.2 Vulnerabilities shall be classified according to risk and remediated in accordance with the Company's vulnerability management process.

9.3 Critical vulnerabilities should normally be remediated within seven days and High vulnerabilities within fourteen days.

10 SECURITY INCIDENT MANAGEMENT

10.1 Where an application security vulnerability or breach is identified, the Company shall assess the impact, contain affected services where appropriate, remediate the issue, notify relevant stakeholders where required and conduct a post-incident review to identify opportunities for improvement.

11 TRAINING, COMPLIANCE AND CONTINUAL SECURITY ASSURANCE

11.1 Developers shall receive secure coding and OWASP awareness training together with regular updates on emerging threats.

11.2 The Company shall undertake regular security audits of software, applications and deployment pipelines and maintain alignment with recognised good practice including ISO 27001 and OWASP ASVS.

11.3 Continual assurance activities may include penetration testing, dependency reviews, access reviews, policy reviews and security testing following significant platform changes.

12 RELATED POLICIES

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

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

13 QUESTIONS ABOUT THIS POLICY

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

support@teamtrack.uk

14 KEEPING THIS POLICY UP TO DATE

14.1 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.

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

14.3 Material changes shall be communicated to all relevant personnel.

Appendix A – Secure Code Review Checklist

☐ Input validation implemented

☐ Authentication and authorisation enforced

☐ No hardcoded secrets

☐ Secure error handling

☐ Dependencies checked for vulnerabilities

Appendix B – Threat Modelling Template

Feature Name:

Assets:

Threats Identified:

Attack Vectors:

Mitigations:

Risk Rating:

Appendix C – Vulnerability Tracking Log

ID:

Severity:

Component:

Date Found:

Remediation Action:

Status:

Owner:

Appendix D – Release Security Checklist

☐ SAST/DAST completed

☐ No critical vulnerabilities

☐ Dependencies updated

☐ Secrets properly managed

☐ Approval obtained