trojan

INFORMATION SECURITY POLICY

POL-002

CLASSIFICATION: PUBLIC

trojan.ie/ (0)71 9662552 info@trojan.ie

Change History

REV	DETAILS OF CHANGES	Effective Date
0.0	FIRST ISSUE	

Current Version:	0	
Release Date:		
Authors:	The Compliance Team	
Reviewers:	Stephen Hennessy & Ciaran O'Connor	
Approvers:	Stephen Hennessy – Operations	Ciaran O'Connor – Commercial Director
Approvers:		

CONTENTS

1. PURPOSE

The purpose of this policy is to define Trojan IT's commitment to information security and to establish the principles and direction for managing information security in accordance with ISO/IEC 27001:2022. This policy supports the organisation's strategic objectives and provides the framework for setting information security objectives and implementing appropriate controls.

2. SCOPE

This policy applies to all information assets, systems, processes, and personnel within the scope of the Information Security Management System (ISMS). The ISMS covers Trojan IT's internal business operations and the design, development, operation, and maintenance of the Thrive software platform.

This policy applies to all employees, contractors, and relevant third parties who have access to Trojan IT information or systems.

3. INFORMATION SECURITY OBJECTIVES

Trojan IT is committed to ensuring that information is protected in a manner that preserves its confidentiality, integrity, and availability. The organisation establishes information security objectives that are measurable, consistent with business needs, and aligned with the ISMS. These objectives are reviewed as part of management review and updated as necessary to support continual improvement.

4. INFORMATION SECURITY PRINCIPLES

Trojan IT commits to the following information security principles:

- Protecting the confidentiality, integrity, and availability of information assets.
- Ensuring information security risks are identified, assessed, treated, and monitored in accordance with SOP-004 ISMS Risk Management.
- Complying with applicable legal, regulatory, contractual, and statutory requirements.
- Embedding information security into business processes, system design, and change activities, including secure development and change control.
- Applying the principle of least privilege and role-based access control to information and systems.
- Maintaining appropriate physical, technical, and organisational security controls.
- Ensuring information security incidents are reported, managed, and learned from.
- Promoting information security awareness and responsibility across the organisation.
- Continually improving the effectiveness of the ISMS.

5. GOVERNANCE AND RESPONSIBILITIES

Top Management is accountable for establishing, approving, and supporting this Information Security Policy and for ensuring that information security objectives are compatible with the strategic direction of Trojan IT.

The ISMS Lead is responsible for maintaining the ISMS, monitoring compliance with this policy, and reporting on ISMS performance to management.

All employees and contractors are responsible for complying with this policy and with all supporting information security policies, procedures, and standards.

6. RISK MANAGEMENT

Information security risks are managed in accordance with SOP-004 ISMS Risk Management. Risks are identified and assessed using a structured methodology and treated using appropriate risk treatment options. Residual risks are reviewed and approved by authorised management.

Risks are reviewed periodically and whenever significant changes occur.

7. CHANGE MANAGEMENT

All changes that may impact information security, including changes to systems, infrastructure, applications, processes, or suppliers, must be assessed, approved, and implemented in accordance with POL-028 Change Management Policy. Security impacts are considered as part of all change activities to prevent unintended degradation of controls.

8. LEGAL, REGULATORY, AND CONTRACTUAL COMPLIANCE

Trojan IT identifies and complies with applicable legal, regulatory, and contractual information security requirements. Compliance obligations are considered during risk assessment, supplier management, and service delivery activities.

9. INCIDENT MANAGEMENT

Information security incidents and suspected weaknesses must be reported promptly and managed in accordance with SOP-006 ISMS Corrective Action and Information Security Incidents. Trojan IT investigates incidents, takes corrective actions, and implements improvements to prevent recurrence.

10. AWARENESS AND TRAINING

Trojan IT ensures that employees and relevant third parties receive appropriate information security awareness training in line with POL-010 Information Security Awareness and Training Policy. Awareness activities are designed to support secure behaviour and understanding of individual responsibilities.

11. MONITORING, REVIEW, AND CONTINUAL IMPROVEMENT

Compliance with this policy is monitored through audits, reviews, and management oversight. The effectiveness of the ISMS and this policy is reviewed as part of management review and internal audit activities in accordance with SOP-007 ISMS Internal Audits.

Trojan IT is committed to the continual improvement of the ISMS and the information security controls that support it.

12. POLICY REVIEW AND APPROVAL

This policy is approved by Top Management and is reviewed at least annually, or sooner if required due to significant changes to the organisation, its operations, or the threat landscape.

Non-compliance with this policy may result in disciplinary action and, where applicable, contractual or legal consequences.