INFORMATION SECURITY POLICY

Version 12.4

June 2025

Table of Contents

GENERAL NOTICE

This document falls under ISMS governance control. The following applies to this document:

- This document is controlled as part of Information Security department;
- No changes to this document are permitted without formal approval from the document owner;
- This document is classified, version controlled and regularly reviewed;
- Any questions regarding this document should be raised to the Information Security Department;
- Distribution, modifications and access must be addressed based on TMF Group's Information Classification;
- The version of this document can be found on the cover page;
- Revision details are described below;
- The governing language of this document is English. Any translations of this document are made for informative purposes only. In case of any inconsistencies, the English version will prevail.

CLASSIFICATION
Public

STAKEHOLDERS	
Owner	Chief Security and Resilience Officer (CSRO)
Reviewer	Information Security Function
Approver	Risk and Compliance Committee (RCC)
Sponsor	Chief Operations and Technology Officer (COTO)

REVIEW	
Period	Annual
Last review	06 June 2025
Status	Final
Approval on	09 June 2025
Effective date	09 June 2025

CONTACT POINT	
Contact	TMF Group ISMS
Details	Contact the team via ISMS@tmf-group.com

1. INTRODUCTION, PURPOSE AND SCOPE

To provide management direction and support for information security in accordance with business requirements, relevant laws and regulations, and the ISO/IEC 27001:2022 standard, this Information Security Policy is defined, approved, published, and made available to all employees, contractors, and relevant external parties.

The Information Security Policy (the “Policy”) is defined to achieve the following objectives:

- To ensure consistent control of information security risks throughout the entire organisation;
- To ensure compliance with all applicable legal, regulatory, and contractual requirements;
- To ensure that information assets and supporting facilities across the organisation are adequately protected in accordance with their associated risk levels;
- To have all its employees and contractors aware of security principles and policies;
- To the extent possible, to maintain oversight of third party service providers to meet TMF group`s information security requirements.

Compliance with the Information Security Policy is mandatory for all employees and contractors. The Information Security Management System (ISMS) documentation consisting of the overarching ‘Establishment of ISMS’ document, along with supporting Standards, Procedures, processes and Guidelines, is made available to all staff through TMF Group’s internal portal. These documents provide the necessary information and guidance to help employees consistently meet the requirements of TMF Group’s ISMS across the organisation.

2. POLICY STATEMENT

TMF Group is committed to implementing adequate information security practices and controls to protect the assets and business interests of TMF Group. This is achieved through the design, implementation, maintenance, and continuous improvement of an Information Security Management System (ISMS). The objective of the ISMS is to ensure the confidentiality, integrity, availability, accountability, and privacy of TMF Group`s information assets which is based on the assessment of information security risks which will enable TMF Group to meet its legal, regulatory, and contractual obligations for its clients and other stakeholders.

All infrastructure used by TMF Group, including servers, workstations, network devices, and applications, is managed in accordance with this Information Security Policy and all supporting standards, procedures, processes and guidelines. This ensures that all systems and platforms across the organization are aligned with the overarching objectives of the ISMS and are consistently secured to minimise risks.

2.1 Principles

- Management is committed to the security objectives and establishes an overall sense of direction and principles for action as described in the 'Establishment of ISMS' document.
- Management is committed to the implementation and maintenance of all relevant security standards, procedures, processes and guidelines. They provide required resources to ensure that the expected level of confidentiality, integrity, availability, accountability, and privacy of information assets are maintained.

2.2 General Requirements

- To initiate and control the implementation and operation of information security within TMF Group, information security roles and responsibilities shall be clearly defined and allocated;
- The ISMS shall be reviewed on at least an annual basis, or whenever major changes occur, and whenever an immediate improvement to the ISMS is required;
- Risks associated with the loss of confidentiality, integrity, and availability for information assets within the scope of the ISMS shall be identified, analysed, and treated on an annual basis;
- TMF Group and all its employees and contractors are bound to comply with the Information Security Policy and all applicable standards, processes, procedures, and guidelines.
- Every individual working within TMF Group is responsible for maintaining the security of the organisation. Each person is accountable for their own compliance and is also expected to support others in fulfilling their security responsibilities.
- As far as the nature of each relationship permits, all principles and rules set out in the Policy shall apply to the relations that TMF Group has with its employees, subcontractors, agents, consultants, interns, and trainees;
- In exceptional circumstances, and with appropriate justification, a security exception may be granted to a specific ISMS policy, process, procedure, or standard. Any granted exception must be supported by appropriate compensating controls.

3. ROLES AND RESPONSIBILITIES

- **Chief Security & Resiliency Officer (CSRO)**

  The Chief Security & Resiliency Officer (CSRO) holds the ultimate responsibility for the organisation's information security.

- **Information Security Governance Risk and Compliance (GRC)**

  The GRC team manages the implementation, maintenance and continuous improvement of the Information Security Management System (ISMS) in accordance with the requirements of the standard.

- **Assurance and Accreditations Management**

  The Assurance and Accreditations team manages the global accreditations programme across the locations in scope within TMF Group.

- **Client Business Security**

  The Global Client Information Security Support team assists stakeholders within TMF Group to manage client information security queries, questionnaires and audits as the primary point of contact for clients seeking clarity on security-related topics.

- **Security Operations Management**

  The key role of this team includes monitoring, detecting and responding to security threats and incidents.

- **Security Project Engineering and Architecture**

  The key role of this team is to design a secured infrastructure as well as to evaluate and recommend security technologies, tools and practices to improve TMF Group's security posture.

- **Third Party Information Security Risk Management (TPRM)**

  The TPRM team ensures that Information Security Risks of TMF Third Party Service Providers are being managed effectively.

- **Business Continuity Management (BCM)**

  The Global BCM team is responsible for the overall BCM implementations and programme.

DEFINITIONS AND ABBREVIATIONS

TERM	DEFINITION
External parties	Any person or entity who contributes to, engages in, or is affected by or concerned with TMF Group
Sub-contractors	Entities providing services on behalf of TMF-Group

REFERENCE TO ASSOCIATED DOCUMENTS

ASSOCIATED DOCUMENTS	
TMF Group – Establishment of the ISMS	Latest version available on the intranet page of TMF Group
TMF Group – Information Security Procedures	Latest version available on the intranet page of TMF Group
TMF Group – Information Security Guidelines	Latest version available on the intranet page of TMF Group
TMF Group – Information Security Standards	Latest version available on the intranet page of TMF Group

REVISION HISTORY AND RECORDS

VERSION	DATE	AUTHOR	DETAILS
1	01-04-2009	Michiel Benda	Initiation of document
2	21-04-2010	Michiel Benda	Annual review – minor changes only
3	05-04-2011	Michiel Benda	Annual review - further integration of sbc policies
4	19-05-2012	Michiel Benda	Update to reflect merger changes and organizational structure
5	26-11-2013	Michiel Benda	Alignment to ISO 27001 ISMS + new corporate layout
5.1	18-02-2016	Michiel Benda	No significant changes
6	27-06-2017	Mike Ward	Refined in-line with s-rm review procedure
7	21-08-2017	Mike Ward	Reviewed with ISO leads
8	22-08-2017	Igor Musial	Updates following review meeting 21/08/2017
9	25-08-2017	Indira Guggisberg Singh	Updates
9.1	15-Mar-2017	Michiel Benda	Initiation of document (new policy library)
9.2	9-Oct-2017	Dan Caplin	First revision for policy restructure
9.3	26-Oct-2017	David Holman	Re-write and review for policy restructure
9.4	27-Oct-2017	Mike Ward	4-eyes review
9.5	17-Jan-2018	Mark Belgrove	Approval and final review
9.6	27-Mar-2018	Mark Belgrove	Document classification simplified and updated
10	17-Sep-2018	Devender Kumar	Section 17 updated to reflect the ISO 27001:2013 requirements for Information Security Aspects of Business Continuity
11	04-July-2019	Devender Kumar	Information Security Policy alignment with TMF Group's policy structure and format
11.1	29-Jul-2019	Devender Kumar	References to TMF changed to TMF Group. Updated control 9.1.4. Prefixed 'information' to assets to explicitly refer to information assets.
12	15-July-2021	Anuj Tewari	Included Policy statement and removed Annex A clauses
12.1	22-June-2022	Anuj Tewari	Annual review; minor changes in Introduction and 2.2 (rephrasing granting of security exceptions)
12.2	10-July-2023	Anuj Tewari, Rohit Rajput	Annual review; minor updates, rephrasing and change in contact point.

VERSION	DATE	AUTHOR	DETAILS
12.3	03-June-2024	Anuj Tewari, Rohit Rajput, Alvaro Guerrero	Annual review with minor updates.
12.4	09-June-2025	Alvaro Guerrero, Jothene Carosin, Rohit Rajput	Annual review with minor updates - including a roles and responsibilities table.