Statement of Continuity

June 2025 | Version 7.7

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 Owner;
- 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;
- This document may be available in various languages; however, the version in the English language will prevail.

CLASSIFICATION
Public

STAKEHOLDERS	
Owner	Chief Security and Resilience Officer (CSRO)
Reviewer	Information Security Function
Approver	Management Board
Sponsor	Chief Operations and Technology Officer (COTO)

REVIEW	
Period	Annual
Last review	06 Jun 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. GOVERNANCE, RISK AND COMPLIANCE

TMF Group recognises the criticality and sensitivity of the services it delivers to clients across the globe. We maintain a robust security assurance framework that integrates people, processes, and state-of-the-art technology, to ensure ongoing security and compliance.

GOVERNANCE

The Executive Committee (ExCo - Senior Management) of TMF Group is ultimately accountable for Information Security at TMF Group. The ExCo approves the Information Security policies, sets security objectives, and provides strategic directions and oversight for all Information security-related aspects of the organization.

The Information Security function, headed by the Chief Security and Resilience Officer (CSRO), is responsible for the implementation, maintenance, monitoring, and review of the Information Security Management System (ISMS).

PLANNING

TMF Group adopts a risk-based approach to Information Security and the risks are assessed periodically. The Information Security function develops and maintains plans and processes, to achieve defined security objectives.

As part of the Technical Design Authority (TDA), the Information Security function validates the security architecture for technology initiatives, ensuring alignment with security-by-design principles.

OPERATIONS

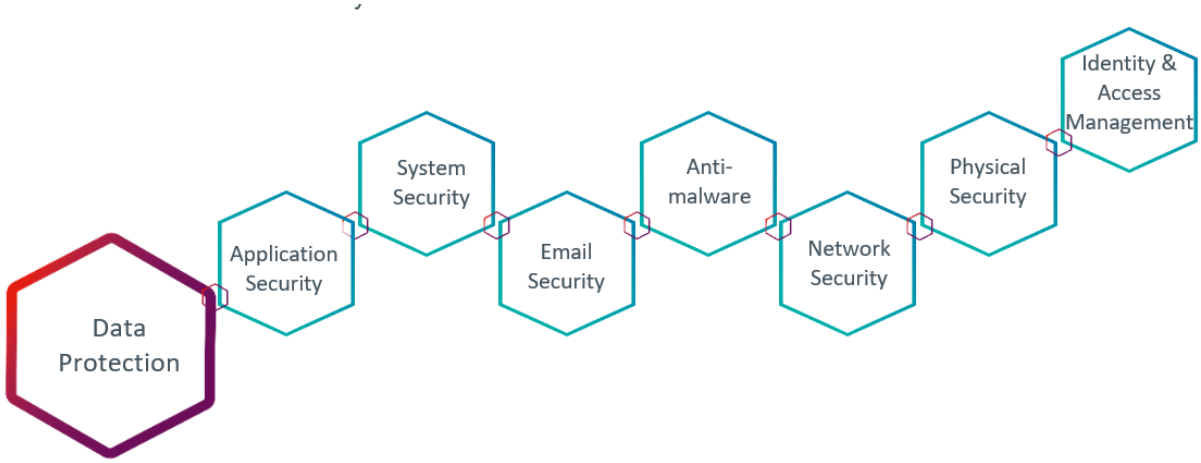
Security Operations focuses on securing TMF Group`s data and network, maintaining compliance with statutory, regulatory, and contractual requirements, and monitoring risks associated with third-party service providers.

A state-of-the-art, round-the-clock Security Operations Centre continuously monitors the TMF Group environment to detect and respond to cyber security incidents. Vulnerabilities across the enterprise technology landscape are regularly scanned and remediated as part of a continuous improvement approach.

A global compliance programme, aligned with ISO/IEC 27001, monitors and maintains the security compliance of TMF offices and data centers. An independent assurance and accreditation programme functions as the third line of defense, providing objective oversight and validation of the effectiveness of security controls

2. DEFENCE-IN-DEPTH APPROACH

At the highest level, TMF Group has established a comprehensive security management framework supported by a set of policies, standards, procedures, processes and guidelines, including, but not limited to, the Business Continuity Management Policy and the Information Security Policy. TMF Group's Information Security Policy is in line with requirements of ISO/IEC 27001 standard. All such documents are made available to all employees through the company's Intranet. A mandatory Group Security Awareness programme is in place to ensure that all employees receive annual training on security policies and practices. Completion of the training is required upon onboarding and refreshed on an annual basis thereafter. All policies are reviewed at least once per year to ensure their continued relevance and effectiveness..



TMF Group adopts a multi-layered security approach encompassing data security, application security, system security, network access controls, monitoring and incident reporting, physical and environmental security, as well as service availability controls.

2.1 Data Protection

TMF Group's data security and protection controls are primarily focused on managing employee access to systems containing client data, ensuring regulatory compliance, and enforcing appropriate user roles and responsibilities.

2.1.1 Data Classification

To understand the sensitivity of information TMF Group has established a standard that classifies data into four categories: Public, Internal, Confidential and Restricted.

This Improved understanding enhances awareness of the potential risks associated with each information category. Consequently, Data Classification allows TMF Group to understand risks associated with information and take appropriate controls to reduce them to an acceptable level.

2.1.2 At rest

'Data at rest' is protected through strict access controls, as outlined in section 2.1.5 Information access. Data is protected through proper access control and logical segregation.

2.1.3 In transit

'Data in transit' is encrypted over public networks. Various technologies are described in this document. For email, this is described in section 2.4. For client access, see section 2.1.6.

2.1.4 Encryption

Encryption is applied to ensure data confidentiality of information where it is deemed necessary, particularly in scenarios involving data mobility or increased exposure risk.

As a mandatory baseline, data at rest is encrypted when stored on laptops, backup systems, or removable media containing client data. These measures are implemented regardless of other risk factors.

In some instances, encrypting data at rest may not be technically feasible due to constraints such as application compatibility or interoperability limitations.

2.1.5 Information access

Access to any information is granted using the principle of 'Least Privilege'. Access control mechanisms are in place to ensure that only authorised personnel may access TMF Group data or client data, as required for business purposes.

TMF Group shall not process, transfer, modify, amend, or otherwise alter Personal Data, nor disclose or permit the disclosure of Personal Data to any third party, except in the following circumstances:

- where necessary to process personal data for the provision of services and/or in accordance with the client`s documented instructions;, or
- where required to comply with Data Protection Laws or other legal obligations applicable to TMF Group, in which case (to the extent permitted by law) TMF Group shall inform the Client of such legal requirement prior to processing.

Information access shall be consistent with TMF Group's Personal Data Protection Policy.

2.1.6 Client access

Bulk file transfers between TMF Group and its clients may be required. To facilitate this, TMF Group provides a secure file-sharing solution that uses strong encryption to protect data during transmission.

Remote access to TMF Group environments by internal users is protected through multi-factor authentication (MFA), which typically involves a user-ID, password, and an additional factor such as a one-time password (OTP) or digital certificate. Access is granted via remote access solutions such as Zscaler and Virtual Desktop Infrastructure (VDI). Zscaler utilizes Single Sign-On (SSO) with device

posture checks, allowing access only from TMF domain-joined systems. VDI (Citrix/AVD) requires username and password with MFA when accessed over the internet. These solutions enforce strict security measures, including endpoint compliance and strong user authentication, to ensure only authorized and secure systems can connect.

Please note that these remotes access solutions are intended for internal use only. TMF Group provides clients with alternative secure channels for data exchange and communication, in line with applicable security and compliance requirements.

2.2 Mobile and teleworking

All company-issued laptops are secured using full-disk encryption to safeguard data in the event of loss or theft. Corporate mobile devices are protected through both mobile application management (MAM) and mobile device management (MDM) technologies, enabling application-level controls such as remote data wiping, data containerisation, and usage restrictions based on security posture. Multi Factor Authentication (MFA) is enforced at the user account level and applies to key corporate applications such as outlook, Teams, and OneDrive, ensuring secure access to critical services and data.

2.2.1 Authentication

Authentication is based on a user-ID/password combination. Passwords must meet defined complexity requirements, including a minimum length and the use of alphanumeric and special characters. Password changes are enforced at regular intervals, and password history controls are implemented to prevent reuse. TMF Group has a formally documented password security standard that is reviewed annually.

Administrative accounts are subject to the same baseline policy as standard user accounts, but must adhere to stricter complexity requirements. Access to administrative accounts is reviewed periodically and is managed through a privileged access management (PAM) solution, which enforces additional security controls and session monitoring.

2.3 Application Security

Application security is reinforced through periodic vulnerability scans and penetration testing, with a focus on the OWASP Top 10 risk categories. Identified vulnerabilities are appropriately assessed and remediated in line with TMF Group's security standards and risk management processes.

2.4 System Security

TMF Group desktops and servers are secured by system hardening, regular vulnerability assessments and a structured patch management process. Security policies based on industry-leading practices are enforced centrally across the environment. Access to systems is controlled and monitored, and audit logs are actively monitored.

2.4.1 Change management

TMF Group has constituted a Change Advisory Board (CAB). The CAB focuses on changes that require careful consideration due to their complexity, potential impact, or associated risk to Business Operations. Such changes are formally reviewed and approved by the CAB Panel and a record of all changes is maintained. The CAB includes representation from Information Security team, to ensure that security considerations are evaluated prior to the implementation of any change presented during CAB meetings. TMF Group follows ITIL v3 best practices for its IT change management processes.

2.4.2 Patch management

Security patches are reviewed, tested and deployed in accordance with the defined patch management process. Patches are applied to systems only after successful testing and appropriate approvals. TMF Group uses a centralised tool to deploy patches across its technology landscape. The Patch management process also includes provisions for the expedited deployment of critical patches in response to specific security advisories or emerging threats.

2.4.3 System Hardening

TMF maintains system hardening standards for key technologies deployed across its technology landscape. These standards are designed to reduce the attack surface by disabling unnecessary services, enforcing secure configurations, and aligning with recognised industry benchmarks.

2.5 E-Mail Security

All incoming and outgoing emails are routed through a secure email gateway that provides protection against malware, spam, phishing & spoofing. TMF Group utilises a cloud-based email security and risk management platform is in place to enhance protection and ensure comprehensive threat mitigation.

Transport Layer Security (TLS) is implemented on the email gateway to encrypt messages in transit. Forced TLS is enforced where supported by clients' systems, ensuring secure and compliant email communication.

2.6 Anti-virus and Malware Protection

Endpoints are protected using next-generation endpoint detection and response (EDR) solutions, that include anti-malware and behavioural analysis capabilities.

2.7 Network Security

TMF Group implements industry best practices in the design, configuration, and operation of its network infrastructure. Enterprise-grade network equipment is used to provide a secure and reliable platform. To support network and infrastructure security, physical access to key IT areas, such as data centres, servers' rooms, and hub rooms is tightly controlled. These areas are located in environments designed to support the safe storage and protection of information, with measures in place to reduce risks associated with fire, temperature, and other environmental factors.

Furthermore, access to these critical areas is restricted through proximity card-based systems, entry and exit points are monitored by CCTV round the clock. Offices have Intruder alarms installed or on-site security personnel during off-hours to detect/prevent unauthorised physical access.

3. Awareness

3.1 Awareness program

TMF Group encourages its employees to keep themselves informed through the Organisation's Intranet. All employees are required to complete the Annual Security Awareness Training programme to ensure a baseline understanding of key information security principles. Important updates regarding security topics and high-risk situations are communicated via special notifications through email, the Intranet, and the internal social network (Viva engage post). Employees are also guided through the TMF Group Code of Conduct, Employee Handbook, onboarding process, and the Mandatory Training Programmes at the beginning of their employment.

4. SECURITY AUDITS

4.1 Vulnerability Assessments

TMF Group performs internal vulnerability scans monthly. The results are consolidated into internal reports for further reviews. Identified vulnerabilities are documented along with their respective actions and justifications. Remediation is prioritised and carried out based on the criticality of each finding.

4.2 Penetration Testing

Annual penetration tests on critical assets are conducted by an independent third party to assess potential vulnerabilities and strengthen TMF Group`s overall cybersecurity posture.

4.3 Security Monitoring

TMF Group operates a round-the-clock monitoring service that collects and analyses event logs from its IT environment using state-of-the-art security monitoring tools. Security Incidents identified by the Global Security Operations Centre (GSOC) are managed in accordance with the defined Information Security Incident Management Process. All relevant logs are retained for a minimum period of 12 months.

4.4 Internal & External Audits

Internal and external audits covering information security are conducted annually, in alignment with the ISO/IEC 27001 standard.

5. HUMAN RESOURCES SECURITY

People are often considered the weakest link in the security chain. The following section outlines the measures implemented by TMF Group to ensure that employees remain aware of and committed to upholding the organisation`s information security principles.

PRIOR TO EMPLOYMENT	Prospective employees are screened prior to employment, by conducting antecedent and referral checks to the extent permitted by law in each country.
ONBOARDING	Employees and contractors are provided with an Information Security awareness briefing at the time of onboarding.
AWARENESS TRAINING	Information Security awareness trainings are aligned to the organization`s core values. Periodic training is provided to staff on behavioral aspects of Security such as information classification and handling, clean-desk clean-screen policy, password security, secure email and internet protocols, malware and phishing attacks, social engineering, security incident reporting among others.
AWARENESS CAMPAIGNS	To sustain the awareness and behavior levels of staff, periodic awareness campaigns and roadshows are conducted.

5.1 Employee Recruitment

TMF Group is committed to hiring and inviting top talent to the organisation and is expecting employees to adhere to high standards of conduct and behaviour. All TMF Group colleagues need to complete a background check as part of the new hire onboarding process. Additional checks may be conducted during employment, where necessary and appropriate. All background screening is carried out in accordance with applicable local laws and regulations.

5.2 Employment Termination

When employees leave the organisation, all previously granted access rights are promptly and properly revoked, to ensure continued protection of business information. All company-assigned devices are retrieved and secured by the IT team, and all access to corporate emails, systems, and business applications is fully disabled.

6. BUSINESS CONTINUITY

Business Continuity features in TMF Group's top priorities. The Management Board and Supervisory Board support the need for robust Business Continuity measures for the benefit of employees, stakeholders, and customers. As most information within TMF Group is processed digitally, the focus of the continuity measures lies in that area.

TMF Group's Business Continuity Management (BCM) aligns with the ISO 22301:2019 standard. The BCM Policy and specific Business Continuity Plans address management, governance, organisational requirements, strategy, resources, response procedures, testing, plan reviews, and awareness. TMF aims to achieve ISO 22301:2019 certification for select offices in 2025 (Regional Delivery Centres), followed by a phased rollout to additional locations.

6.1 Resilience

TMF Group uses various geographically distributed commercial and local offices data centres where all critical applications are hosted. All connectivity between the commercial data centres is redundant to ensure high availability and near continuous uptime.

All critical network components are internally redundant (dual power supplies, dual network interfaces, etc.). Essential equipment is connected to uninterruptible power supplies which are subject to regular testing and lifecycle refresh to ensure ongoing operational resilience..

6.2 Backups

TMF Group performs daily backups of its data which are retained for a period of four weeks. Monthly and yearly backups are maintained, with yearly backups retained for the maximum duration as legally permitted under applicable local legislation. To ensure the availability and integrity of backup data, backup tapes are encrypted and stored with certified professional storage providers specialising in tape and cloud-based solutions, wherever feasible.

6.3 Accessibility

TMF Group utilises a robust and secure network solution to enable connectivity between offices. This solution allows authorised communication and collaboration across locations and, for continuity purposes, provides the capability to services clients from alternative TMF Group offices worldwide.

In addition, the organisation provides a secure remote access solution that enables employees .to connect to their work environment from virtually any location worldwide. The remote environment is encrypted, and access is secured through multi-factor authentication to ensure confidentiality and integrity.

6.4 Retention

TMF Group has the obligation to have data available, in accordance with local legal requirements. In majority of cases, this obligation remains even after the service to a client has ended. TMF Group ensures that all data is retained as long as it is legally required by the local legislation.

6.5 Health and Safety

As corporate responsibility is a key value of the TMF Group, the organisation cares for the welfare, health and safety of its employees, clients and visitors within its offices.

Managing Health and Safety is also considered as an integral part of the risk management of TMF Group. For these reasons, Health and Safety are key priorities for the organisation.

6.6 Environmental Awareness and Sustainability

TMF integrates environmental considerations into its risk management and continuity planning. The organisation promotes responsible IT resource usage, electronic waste recycling, and initiatives to reduce its carbon footprint.

7. INDUSTRY BENCHMARKS

We constantly benchmark ourselves with the industry leading processes.

ISO 27001 CERTIFICATION	ISAE 3402 SOC1 TYPE 2 AUDITS	BITSIGHT SECURITY RATING
All of our offices comply with the Standard, and the majority have obtained official certification. .	TMF Group has in place an ISAE 3402 SOC 1 Type 2 audit programme in most of the offices, to ensure independent validation of our key IT controls and processes and to help clients meet regulatory and compliance requirements.	BitSight Security Rating is an independent benchmark of an organisation's cyber security performance, assessing external-facing interfaces and its security performance. TMF Group uses BitSight rating to benchmark its Cyber Security posture in line with the industry.

DEFINITIONS AND ABBREVIATIONS

TERM	DEFINITION
CAB	Change Advisory Board
CSRO	Chief Security and Resilience Officer
ExCo	Executive Committee
GSOC	Global Security Operations Centre
HR	Human Resources
ISMS	Information Security Management System
KPI(s)	Key Performance Indicator(s)
MAM	Mobile Application Management
MFA	Multi-factor Authentication
OTP	One-time Password
TDA	Technical Design Authority
TLS	Transport Layer Security
SOC	Security Operations Centre
EDR	Early Detection and Response

REFERENCE TO ASSOCIATED DOCUMENTS

ASSOCIATED DOCUMENTS	
TMF Group – Information Security Policy	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 – Establishment of the ISMS	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	12-Aug-2010	Michiel Benda	Initiation of document
2	30-Nov-2010	Michiel Benda	Additional
3	30-Aug-2011	Michiel Benda	Additional
4	17-Mar-2013	Michiel Benda	Version based on merger
4.1	21-Feb-2014	Michiel Benda	Minor rewording, no new version applied.
5	05-Mar-2015	Michiel Benda	Update to reflect improvement in IT security and ISO compliance
6	20-Jun-2017	David Holman	Review post-restructure
6.1	22-Jun-2017	Mark Belgrove	Minor changes to password length/complexity requirements
6.2	19-Jul-2017	Mark Belgrove	Added risk to organisation structure
6.3	07-Sep-2018	Devender Kumar	Organisation structure updated 9.3 Internal & External Audits included
7.0	13-Sep-2019	Devender Kumar	Document structure and graphics revised; no material changes
7.1	19-Jul-2020	Nitin Dhande	Added section 2.1.1, 2.1.10 and 2.3.3
7.2	09-Dec-2021	Anuj Tewari	Reviewed with RSO's, and CSRO, made amendments in 2.1.4, 2.3.3, 5.1, 6.4 and minor changes.
7.3	01-Jul-2022	Anuj Tewari	Annual review with minor changes on 2.1.4; 2.1.5 2.1.9 and 4.4, 6.3
7.4	27-Apr-2023	Group Risk & Compliance	Minor changes that reflect the new setup of TMF's two-tier board
7.5	19-Jul-2023	Anuj Tewari, Rohit Rajput & Alvaro Guerrero	Annual review; minor updates and rephrasing
7.6	03-Jun-2024	Subhodh Subramanian, Saurabh Gugnani, Jothene Carosin, Rohit Rajput & Alvaro Guerrero	Annual review; minor updates and rephrasing
7.7	09-June-2025	Jothene Carosin, Subhodh Subramanian, Alvaro Guerrero, Rohit Rajput, Cornel Stoian, Vinay Lakhanpal, Vishal Kawle, Taranjit Kaur, Ajay Singla	Annual review with rephrasing of policy content to enhance clarity on security controls. Application names were replaced with general references to systems or services for consistency.