TMF GROUP

STATEMENT OF CONTINUITY

Security and Business Continuity Overview

July 2022 | Version 7.3

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	Information Security Department
Reviewer	Chief Security and Resilience Officer (CSRO)
Approver	Risk and Compliance Committee (RCC)
Sponsor	Chief Operations and Technology Officer

REVIEW	
Period	Annual
Last review	22 June 2022
Status	Final
Approval on	1st July 2022
Effective date	1st July 2022

CONTACT POINT	
Contact	Information Security Department
Details	Contact the team via security@tmf-group.com

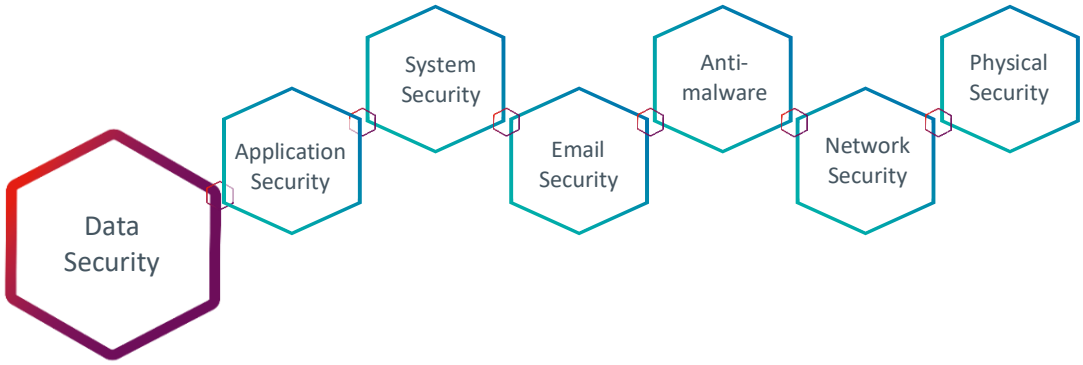
1. GOVERNANCE, RISK AND COMPLIANCE

TMF Group understands the criticality and sensitivity of the services it provides to its clients across the world. We have a robust security assurance framework that combines people, process, and state-of-the-art technology, to ensure we are secure and compliant.

GOVERNANCE	The Executive Committee (ExCo - senior management) of TMF is ultimately accountable for Information Security at TMF Group. The ExCo establishes the Information Security policies, defines security objectives, and provides strategic directions and steer for all security-related aspects of the organisation. The Information Security Department, 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), based on the ISO 27001 standard.
PLANNING	We follow a risk-based approach to Information Security. External and internal risks are assessed periodically and reviewed. The Information Security department prepares detailed plans and processes, to achieve defined security objectives. As part of the Technical Design Authority (TDA), the Information Security Team vets the security design for all technology initiatives, metrics, and Key Performance Indicators (KPIs) for key processes.
OPERATIONS	Security Operations focuses on securing our data and network, maintaining compliance to statutory, regulatory, and contractual requirements and monitoring risks from third party service providers. A state-of-the-art, round the clock Security Operations Centre monitors the TMF Group network, to detect and respond to cyber security incidents. Vulnerabilities in the enterprise technology landscape is scanned and remediated on an ongoing basis. A global compliance program, aligned to ISO 27001, monitors, and maintains security compliance of TMF offices and data centre. An independent Internal Audit program acts as the third line of defense.

2. DEFENSE-IN-DEPTH APPROACH

At the highest level, TMF Group has drawn up a security management framework and a number of policies, standards, procedures and guidelines including, but not limited to, a Business Continuity Management Policy and an Information Security Policy. TMF Group's Information Security Policy is in line with requirements of ISO27001 standard. These policies, standards, procedures and guidelines are made available to all employees through the company's Intranet. A Group Security Awareness program is implemented to address annual training on the policy awareness for all employees. All policies are reviewed at least annually.



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

2.1 Data Security

TMF Group's data security and protection controls focus on employee access to systems that house client data, regulatory compliance, and user roles.

2.1.1 Data Classification

To understanding the sensitivity of information TMF Group has defined the standard to address the data into Public, Internal, Confidential and Restricted category. Improved understanding leads to a

higher awareness of potential risks associated with specific information classes. Consequently, Data Classification allows TMF Group to understand risks associated with information and take appropriate measures in bringing the risks to an acceptable level.

2.1.2 At rest

'Data at rest' is protected through restrictions on the access rights as described 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 the Internet. 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

TMF Group will use AES–256 level encryption or higher, where encryption is applied. Data is encrypted at rest when data is mobile like in the case of laptops, backups and any removable media that stores client data. It should be noted that not all data at rest is encrypted but at a minimum data is encrypted at rest when stored on laptops, backups and any removable media that stored client data. It may not be possible to encrypt data-at-rest due to limitations related to application compatibility or interoperability.

Information access

Access to any information is granted using the principle of 'Least Privilege'. Approvals for access are given by Information Owners and shall be documented.

TMF shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than:

- as necessary to process Personal Data to provide the Services and/or otherwise in accordance with the documented instructions of Client, or
- as required to comply with Data Protection Laws or other laws to which TMF is subject, in which case TMF shall (to the extent permitted by law) inform Client of that legal requirement before processing the Personal Data.

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

2.1.5 Client access

Bulk file transfers may be needed between TMF Group and its clients. TMF Group offers an additional service to provide secure file-sharing through TMF Group ShareFile, a commercial solution using strong encryption.

2.1.6 Remote access

Remote access requires multi-factor authentication, usually consisting of user-ID, password, and a certificate or another factor like OTP (One Time Password). Remote access is done through VPN or remote desktop technologies.

2.1.7 Mobile and teleworking

All laptops are encrypted with AES 256. Mobile Application Management (MAM) has been implemented to protect data on mobiles which includes remote wipe capabilities. Multi Factor Authentication (MFA) is required on mobile phones.

2.1.8 Authentication

Authentication is based on a user-ID/password combination. Passwords must meet complexity requirements that mandate a minimum number of characters and must contain alphanumeric as well as special characters. Password change at regular intervals and password history is also enforced. TMF Group has a formally documented password security standard that is reviewed at least annually.

Administrative accounts follow the same password policy as regular accounts but require a password with higher complexity requirements. There are a limited number of system administrators in possession of the administrative account details. Admin access is reviewed periodically.

2.1.9 Data Disposal

All information goes through an information lifecycle. At the end of that lifecycle, the underlying data is disposed of. Especially on digital storage, data that is seemingly disposed of might still be accessible through semi-advanced technologies. To avoid information disclosure in this way, TMF Group has defined strict data and media disposal processes.

2.2 Application Security

Periodic vulnerability scans based on OWASP Top 10 vulnerabilities and penetration tests are conducted and appropriately remediated.

2.3 System Security

TMF Group desktops and servers are secured by hardening, vulnerability assessments and patch management processes. Security policies based on industry-leading practices are enforced centrally. Accesses and audit logs are monitored.

2.3.1 Change management

TMF Group has constituted a Change Advisory Board (CAB). All technology changes have to be approved by CAB. A record is maintained for all changes. CAB includes representation from Information Security team, to ensure information security aspects are reviewed before rollout of any change. TMF Group follows ITILv3 best practices for its IT Change Management processes.

2.3.2 Patch management

Security patches are reviewed and tested. Patches are applied to the systems after testing and due approvals as per process. TMF Group has deployed a tool to push patches to its workstations and servers. Patch management process addresses the requirements for critical patch rollout as may be needed, as a result of specific security advisories.

2.3.3 System Hardening

TMF maintains Hardening standards for key technologies that are utilised in its technology landscape.

2.4 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 has enabled TLS (Transport Layer Security) on its mail gateway to encrypt email during transit. Forced TLS is available wherever supported by clients.

2.5 Anti-virus and Malware Protection

The servers and workstations are protected through next gen endpoint detection and response software.

2.6 Network Security

TMF Group implements industry best practices in the design and configuration of its network and utilises industry leading network equipment to provide a secure and reliable platform.

The TMF Group networks are protected through multiple firewall layers. Perimeter protection is constantly being reviewed to ensure that breaches are highly unlikely. Quarterly vulnerability scans of the network perimeter are conducted and actioned accordingly.

2.7 Physical Security

All strategic data centres are housed in fire-proof rooms. The offices are equipped with climate control systems, early warning and detection systems and appropriate extinguishing equipment. Furthermore, critical areas such as the server room and main entrances are protected using a proximity card-based access control system. CCTV equipment monitors these areas on a 24x7 basis. Offices have Intruder alarms installed or physical guards on duty during off-hours to detect/prevent unauthorised access to the premises.

3. AWARENESS

3.1 Awareness program

TMF Group encourages its employees to keep themselves informed through the Organisation's Intranet. All employees are expected to go through an annual Security Awareness Training program. Special notifications by email and through the Intranet ensure that all employees are made aware of changes in security and high-risk situations. Employees are guided through the TMF Group Code of Conduct, Employee Handbooks, Induction Sections and Mandatory Trainings Programmes at the beginning of their employment.

4. SECURITY AUDITS

4.1 Vulnerability Assessments

TMF Group performs quarterly internal and external vulnerability scans. The results of the scans are aggregated into an internal report. Actions and justifications of the potential vulnerabilities are recorded, and remediation is done based upon the criticality.

4.2 Penetration Testing

Annual penetration tests on all public IPs and internet facing applications are conducted by an independent third party.

4.3 Security Monitoring

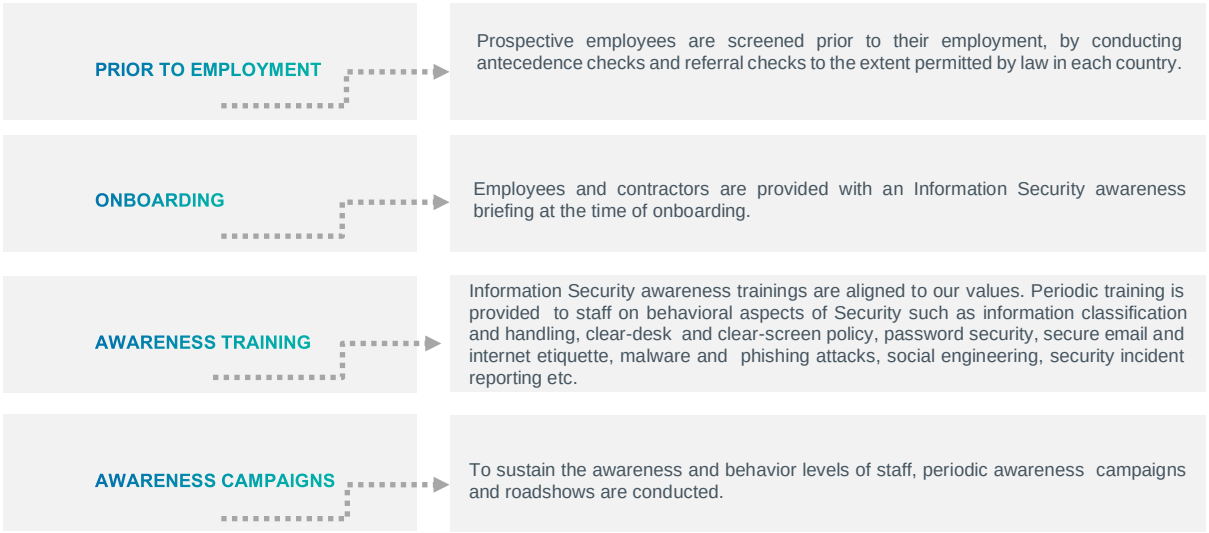
TMF Group has a round the clock monitoring service that collect and analyses the event logs from TMF Group's IT environment. TMF Group has deployed state of the art tools for security monitoring. Incidents identified by the Global Security Operations Centre (GSOC) are addressed per defined Security Incident Management Procedure.

4.4 Internal & External Audits

Internal and external audits are conducted at least annually covering Information Security based on ISO 27001 standard.

5. HUMAN RESOURCES SECURITY

People are often the weakest link in the security chain. Here is an overview of the measures taken at TMF Group to keep the workforce committed to security.



5.1 Employee Recruitment

TMF Group is committed to hiring and attracting 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. Employees may also be asked to complete further checks as and when required. All background checks will be carried out in accordance with local law and legislation.

5.2 Employment Termination

When employees leave the organisation, all previously granted access rights are promptly and properly revoked, ensuring access to the business information is safeguarded.

6. BUSINESS CONTINUITY

Business Continuity features in TMF Group's top priorities and the TMF Group Board supports 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.

6.1 Resilience

TMF Group uses various geographically spread commercial data centres where all critical applications are hosted. All connectivity between the data centres is redundant to ensure near 100% uptime.

All critical network components are internally redundant (dual power supplies, dual network interfaces, etc.). Critical equipment is attached to UPS's that are regularly tested and refreshed.

6.2 Backups

TMF Group makes daily backups of all its data. Daily backups are retained for four weeks. Monthly and yearly backups are in place. Yearly backups are retained for a maximum period as legally permitted in the local legislation. To ensure that backups are available at all times, backup tapes are encrypted and stored at certified, professional storage companies, specialising in tape storage (wherever possible).

6.3 Accessibility

TMF Group utilises a robust and secure network solution for providing connectivity. This solution allows offices to communicate with each other and, where necessary and authorised. For continuity purposes this solution offers TMF Group the opportunity to service its clients from any other location in the world.

In addition, the organisation has a secure remote access solution. This remote access solution allows employees to access their work environment from virtually any location in the world. The environment is encrypted and access is based on a multi-factor authentication.

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.

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 our offices are aligned to the standard, with almost all offices certified against the Standard.	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

REFERENCE TO ASSOCIATED DOCUMENTS

BUSINESS CONTINUITY POLICY	TMF GROUP POLICY LIBRARY
Code of Conduct	TMF Group Policy Library
Establishment of ISMS	TMF Group Policy Library
Information Security policy	TMF Group Policy Library

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	30-08-2011	Michiel Benda	Additional
4	17-03-2013	Michiel Benda	Version based on merger
	21-02-2014	Michiel Benda	Minor rewording, no new version applied.
5	05-03-2015	Michiel Benda	Update to reflect improvement in IT security and ISO compliance
6	20-06-2017	David Holman	Review post-restructure
6.1	22-06-2017	Mark Belgrove	Minor changes to password length/complexity requirements
6.2	19-07-2017	Mark Belgrove	Added risk to organisation structure
6.3	09-2018	Devender Kumar	Organisation structure updated 9.3 Internal & External Audits included
7.0	13-09-2019	Devender Kumar	Document structure and graphics revised; no material changes
7.1	19-07-2020	Nitin Dhande	Added section 2.1.1, 2.1.10 and 2.3.3
7.2	09-12-2021	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	01-07-2022	Anuj Tewari	Annual review with minor changes on 2.1.4; 2.1.5 2.1.9 and 4.4, 6.3