Global reach
Local knowledge

STATEMENT OF CONTINUITY

Security and Business Continuity outline

18 October 2018 | Version 6.3

tmf-group.com

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 quality assurance;
- 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 Data Classification Policy;
- 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 Information Security Officer
Approver	TMF Group Board
Sponsor	Chief Information Officer

REVIEW	
Period	Annual
Last review	03 September 2018
Status	Final
Approval on	18 October 2018
Effective date	18 October 2018

CONTACT POINT	
Contact	-
Details	-

SUMMARY

TMF Group acknowledges the importance of its clients and the dependency its clients have on the services our organization provides. This acknowledgment has led TMF Group to make large investments in both security and business continuity solutions.

This statement gives a brief overview of the measures we have taken to maximize the continuity of services to your organization, to minimize the duration of any disruptions and to protect our assets as well as all assets entrusted to us by our clients.

1. INTRODUCTION

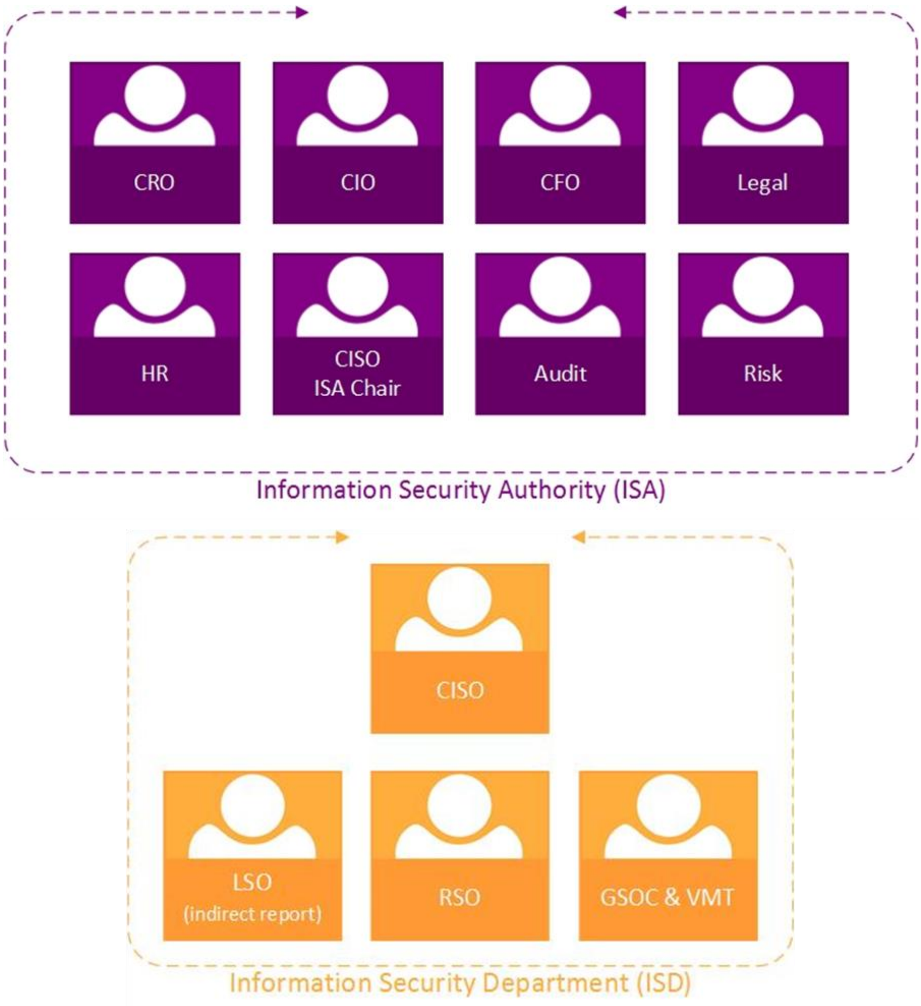
TMF Group acknowledges the importance of its clients and the dependency its clients have on the services our organization provides. This acknowledgment has led TMF Group to make large investments in both security and business continuity solutions.

This statement gives a brief overview of the measures we have taken to maximize the continuity of services to your organization, to minimize the duration of any disruptions and to protect our assets as well as all assets entrusted to us by our clients.

It should be noted that TMF Group is a dynamic organization, as is the environment in which it operates. Consequently, TMF Group reserves the right to update its security and continuity environments without consulting or pre-informing its clients. TMF Group guarantees that any changes made to this environment will at least conform to industry expected practices. Clients may retrieve the latest version of this Statement from the TMF Group website to match their own requirements against those implemented by TMF Group.

2. ORGANIZATION STRUCTURE

In recognition of the importance of both Security and Business Continuity, TMF Group has a dedicated Information Security governance structure as depicted below.



The Information Security Authority (ISA) defines the strategic direction for all Information Security related aspects of the organization and gives final approval of the policies. The Information Security Department is responsible for day to day information security related operations in the organization.

3. POLICIES

At the highest level, TMF Group has drawn up a security management framework and a number of policies, amongst which a Business Continuity Management Policy, an Information Security Policy (ISO 27001 compliant), and a Health and Safety Policy. These policies 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 on a regular basis, mostly annually.

The majority of policies, processes and procedures of the TMF Group organization are classified as Internal. Consequently, these policies, process descriptions and procedures may not be distributed outside the TMF Group organization.

4. CORPORATE RESPONSIBILITY

TMF Group sets high value on being a good corporate citizen. Its position and actions towards corporate responsibility reflect this, and TMF Group ensures that every aspect of its business is in line with this value.

TMF Group defines corporate responsibility as actions taken by TMF Group which positively impact on its customers, investors, people, suppliers and the communities around its businesses beyond its legal and regulatory obligations. The organization's Code of Conduct, which is signed by all employees, is just one of the measures in this responsibility that TMF Group has taken. Our Corporate Responsibility statement can be found here.

5. HEALTH AND SAFETY

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

Managing health and safety is also considered an integral part of the total risks management of TMF Group. For these reasons, Health and Safety are key priorities for the organization. This is further translated into the organization’s first aid program, pandemic program and evacuation procedures.

6. SECURITY

6.1 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 badge-based access control system. CCTV equipment monitors these areas on a 24x7 basis. In many offices, physical guards are on duty during off-hours to prevent/detect unauthorized access to the premises.

6.2 Information Security

6.2.1 Storage

Client information is stored only on the company networks, not on workstations. Where an exception needs to be made, a security exception is raised with the ISD. In exceptional cases laptops may contain client information, however all TMF Group laptops are encrypted.

6.2.2 E-Mail

Email is managed by TMF. Email communications with clients are done through Internet-based email transfers. Wherever the clients support it, TLS is used to encrypt email in transit. All incoming and outgoing emails are routed through a secure email gateway that provides protection against malware, spam, phishing & spoofing. End-to-end email encryption is available as an extra service where requested.

6.2.3 Anti-virus protection

The servers and workstations are protected through next gen anti-virus software which is updated no more than a few hours after the anti-virus solution provider releases new anti-virus signature files.

6.2.4 Network perimeter protection

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

6.2.5 Data Protection

6.2.5.1. At rest

Data at rest is protected through restrictions on the access rights as described in section 6.2.6 Information access. Data is protected through proper access control and logical segregation.

6.2.5.2. In transit

Data in transit is encrypted wherever possible. Various technologies are described in this document. For email, this is described in section 6.2.2. For client access, see section 6.2.77. Remote access is done through an SSL-VPN as described in section 7.3 or through Microsoft's Direct Access.

6.2.5.3. In use

Data is stored by default on the networks. As a consequence, data in use is protected in much the same way as data at rest. In exceptional cases laptops may contain client information, however all TMF Group laptops are encrypted to protect the data in the event of theft.

6.2.5.4. Encryption

TMF Group will use AES-256 level encryption or higher where encryption is applied. Exceptions are noted where systems required to provide the services cannot support this encryption level. It should be noted that not all data at rest is encrypted. Data is encrypted at rest in case of laptops and backups. Local restrictions and application support consequences are two key reasons it may not be possible to encrypt data at rest.

6.2.6Information access

Access to any information is granted using the Principle of Least Privilege. Approvals for access are given by management only and always in writing.

TMF Group does not use any client confidential data that is accessed, stored or passed through their systems, other than in delivery of the service to its clients. Data processed at the request of the client remains the property and responsibility of the client.

6.2.7 Client access

In some situations, file transfers between TMF Group and clients are required that are not done through email. In such situations, TMF Group offers an additional service to provide secure file sharing through TMF Group Share, a commercial solution using strong encryption. Alternatively, non-private cloud-based solutions supported by the client may be accepted after a review and approval from TMF Group Information Security.

6.2.8 Authentication

6.2.8.1. Internal

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 & special characters. Password change at regular intervals & password history is also enforced. TMF Group has a formally documented password policy that is reviewed annually.

6.2.8.2. Remote

Remote access requires 2-factor authentication usually consisting of User-ID, password and token or certificate.

6.2.8.3. Administrative accounts

Administrative accounts follow the same password policy as regular accounts but require a password with higher character length. There are a limited number of system administrators in possession of the administrative account details. Administrative exceptions are registered and individually authorized.

6.2.9Use of Open Source software

TMF Group strives to give clients the highest quality. As a result, it requires the use of Open Source software in some jurisdictions to be able to offer this quality. In practice, this usually means that the application required for the client's data processing requires a Linux-based OS foundation, although there are some jurisdictions where some local reports are generated through Open Source applications.

TMF Group does not develop or modify the Open Source applications it uses and as such is not a contributor to the Open Source Community. TMF Group has support agreements for all Open Source applications that the organization uses to perform its business services.

7. 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.

7.1 Resilience

TMF Group has various geographically spread Tier-3 or higher graded data centres where all critical central data is stored. The data in these centres is synchronized on a real-time basis. 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.

7.2 Backups

TMF Group makes daily backups of all its data worldwide. Daily backups are retained for 5 weeks; monthly 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, stored at certified, professional storage companies, specializing in tape storage wherever possible.

7.3 Accessibility

TMF Group has a high-end private backbone-based VPN solution around the globe. This solution allows all offices to communicate with each other and, where necessary and authorized, work in each other's environment. For continuity purposes this solution offers TMF Group the opportunity to service its clients from any other location in the world.

In addition, the organization 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 fully encrypted, and access is based on a two-factor authentication.

7.4 Retention

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

Due to the nature of the tape backups that TMF Group uses, data for multiple clients as well as the TMF Group internal data may be stored on a single tape (collection).

8. CHANGE MANAGEMENT

8.1 ITILv3

TMF Group follows ITILv3 best practices for its IT Change Management processes.

8.2 DTAP

TMF Group adheres to the various levels of the DTAP (Development, Testing, Acceptance, Production) cycle when managing changes, depending on the complexity and impact of the change. In all business-as-usual situations, any change to any system is reviewed in a test environment.

8.3 Emergency Changes

TMF Group may get approval to skip the testing, provided clear and undisputed roll-back plans have been submitted, and that subsequent testing be performed after the change is made.

8.4 Patch Management

Security patches are reviewed with priority and after proper testing are distributed to the systems for which they are relevant. Patches are assessed and tested before rollout.

9. AUDITING

9.1 System vulnerability scanning

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

9.2 Security Monitoring

TMF Group has a 24x7 monitoring service that collect and analyses the event logs from TMF Group's IT environment. Incidents identified by the Security Monitoring Team are registered and escalated to relevant expert engineers.

9.3 Internal & External Audits

Internal and external audits are conducted annually.

9.4 Human Resource Management

9.4.1 Employee Recruitment

Employee recruitment checks are done in accordance with local requirements and restrictions. Depending on the seniority and responsibility of the role, TMF Group extends the background checks. At the very minimum, the checks include identity verification, reference verifications and certificate verifications. Additional checks may be done where permitted in local legislations.

HR communicates the recruitment of new employees and informs the IT department of the access rights that must be given.

9.4.2Employee Termination

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

10. AWARENESS

10.1 Awareness program

TMF Group stimulates its employees to keep informed through the organization’s intranet. Employees are guided through the Code of Conduct and Employee Handbooks and follow basic induction programs at the beginning of their employment. Special notifications by email and through the Intranet ensure that all employees are made aware of changes in security and high-risk situations. Additionally, all employees are expected to go through an annual security awareness training.

ASSOCIATED DOCUMENTS

RELATED POLICIES		
Code of Conduct	Information Security Policy	Establishment of the ISMS

VERSIONS

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	07-09-2018	Devender Kumar	Organization structure updated