CYBER SECURITY STATEMENT

1. Purpose

As a digital company with an extensive network of stakeholders and a vast repository of data, TM is responsible for safeguarding its assets against all forms of evolving cyber threats. In this regard, we are committed to protecting our stakeholders' interests by putting in place strategies to ensure data integrity and confidentiality.

This statement demonstrates TM's commitment to maintain the highest levels of cyber resilience, via robust governance structures, effective cyber security measures, supply chain management, adherence to internationally recognised cyber security standards, and employee training and awareness programmes.

2. Governance

We have introduced and enforced a Group-wide TM Cyber Security Directive that defines cyber security as a prerequisite for all our solutions design, development, implementation and operations, without compromising user experience. This is to ensure cyber resilience and enhanced data protection in our digitalisation efforts, and compliance with relevant laws, in particular the Communications and Multimedia Act 1998 and Personal Data Protection Act 2010. Compliance to this Group-wide directive is facilitated via our internal Information Security Policy, frameworks**,** guidelines and governing platforms, and is consistent with international standards.

TM internal governance platforms provide oversight on the risk assessment and treatment, as well as effectiveness and compliance of the controls that are deployed. To this end, cyber security risks are monitored and reported on a regular basis to the Group's Board Risk and Investment Committee, and where necessary escalated to TM Board for review and/or relevant decision-making.

2.1 TM Information Security Policy

TM's Group-wide Information Security Policy specifies the guiding principles and responsibilities to safeguard the security of our information assets, both physical and virtual, whilst ensuring the confidentiality, integrity and availability in accordance with the requirements of information security standards ISO/IEC 27001 Information Security Management System (ISMS).

2.2 Certifications

TM has obtained and maintained international certifications that comply with requirements for relevant parts of our operations.

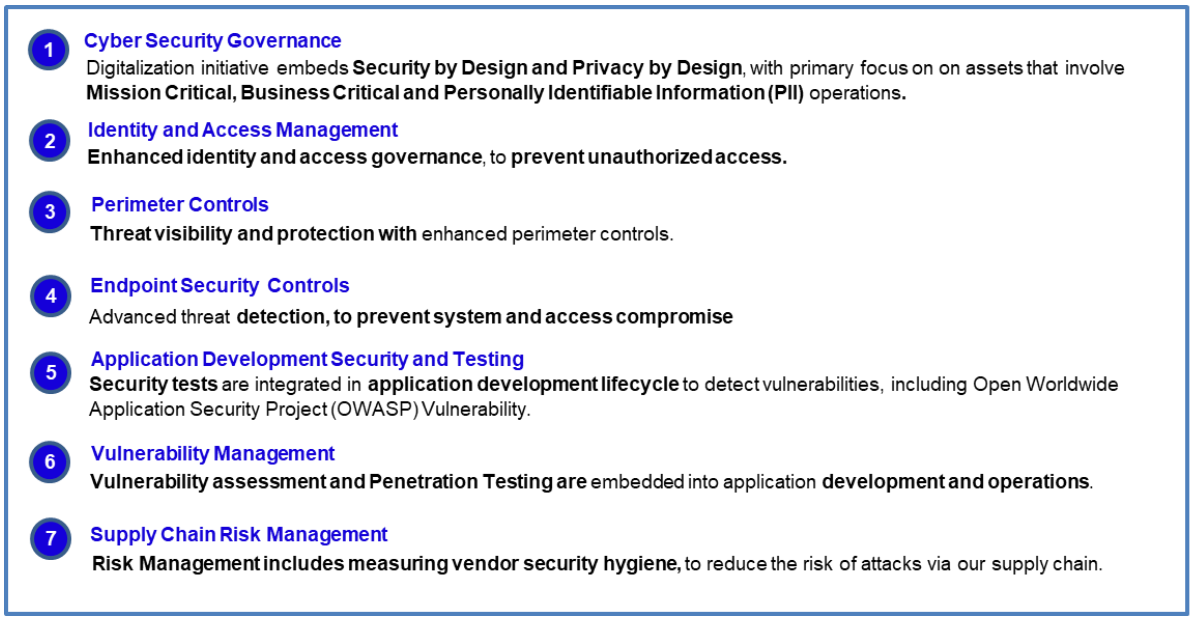
TM maintains ISMS certification and ISO 23301 Business Continuity Management System (BCMS) for IT, Network and Security Operations as well as PCI DSS certification for TM Payment Gateway.

Multiple Certifications are maintained for key services offered to customers. Refer to this link for our certifications.

3. Cyber Security Approach

3.1 Cyber Security Essential Measures

TM is committed to continuous assessment and improvement of the cyber security maturity level of the organisation. In this regard, TM has established essential cyber security measures that are addressed in our Cyber Security Baseline covering seven (7) cyber security domains. These measures are aligned to ISO/IEC 27001 and the National Institute of Standards and Technology (NIST) Cyber Security Framework, providing essential security controls encompassing cyber security architecture requirements, development, implementation and operation in digitalization.



With the various levels of enhanced cyber security controls implementation, we are committed to greater focus on threat visibility, integration and automation. To enable protection of data and the ecosystem against emerging threats, we continuously enhance measures to reduce our threat exposure while fortifying data protection.

3.2 Incident Management

Cyber resilience involves embedding the ability to anticipate, withstand and recover from adverse cyber events or attacks. TM's enhanced internal policies and incident response playbooks undergo periodic exercises to enable a consistent and effective approach to manage information security incidents Group-wide, including communications about security events and vulnerabilities, and learnings from each incident.

3.3 Supply Chain Risk Management

TM works with its key suppliers to enable alignment with our essential security measures. A Vendor Security Index is in place to assess suppliers' security maturity level. The Index is designed to identify continuous improvement opportunities in security measures across all key products and services. We also require suppliers to continuously monitor and mitigate their risks within our supply chain.

3.4 Cyber Security Awareness and Training (Acculturation)

We conduct regular awareness and training programmes to cultivate a cyber-vigilant workforce. These include:

a. Regular Electronic Direct Mail (EDMs) with tips and reminders on protecting information assets
b. Sophisticated phishing simulation exercises to enhance employees' ability to detect scams/phishing attacks
c. Cyber security month featuring online and face-to-face cyber security talks, demonstrations and hands-on activities to increase awareness.
d. E-learning refresher modules on cyber security
e. Table Top Exercises and cyber drills across business and support divisions to enable alignment in incident response and disaster recovery

Employees involved in application development are provided advanced training to enhance their competencies in securing web applications. Focused training programmes are also conducted for Lead Application Developers, on secure Software Development Life Cycle Framework to prioritise cyber security features in all projects.

END