TERRA MAURICIA LTD

Information Technology Policy
(Version 2020 - V1.2)

For the future. From 1838

terra

Governing security measures and technologies implemented at Terra to protect its IT assets.

1. Foreword

This document provides an overview of the security-related technologies and security measures that are in place at Terra to secure its IT assets (data, network, server infrastructure and end-points).

Terra may be referred to as 'the Group', the procedure may be referred to as 'the document' and Information Technology (IT) may be referred to as 'systems', 'information systems' or 'services' in the remainder of this document.

2. Context

Organisations are increasingly relying on Information Technology to conduct their business operations. The Internet is nowadays a major communication channel with the external world and has become an essential element of the business eco-system. But, at the same time it has provided a new arena for criminals to perform malicious activities.

Indeed, organisations are increasingly being the target of cybercriminals whose actions can range from reputational damage to complete loss of business. particularly if adequate security measures are not carefully implemented. With time, cybercriminals' actions have become more sophisticated through the use of advanced tools and tactics which can deceive an organisation vigilance.

This situation has prompted organisations to address risks related to cyber-threats and security breaches as a top priority. Terra has always adopted a proactive approach in terms of cyber security by carefully investing in advanced and reputed security technologies. As such, numerous technologies and measures have been implemented to protect the organisation from different forms of cyber threats.

The purpose of this document is twofold. Firstly, it describes the current cyber threat landscape in which businesses are evolving. Secondly, it provides an overview of the security measures and technologies that have been implemented at Terra to protect its IT assets.

It is important to note that most IT security technologies and measures are purposely "transparent" to end-users.

Moreover, the Group IT Department is keeping pace with the fast changing threat landscape and strives to communicate with end-users when a new threat is identified in order to raise the awareness of end-users, but also to remind about behaviours to adopt when facing a potential threat.

This document does not supersede any existing or future policies, manuals, code of ethics, code of conduct, procedures or other agreements that the Group may define as it sees fit.

3. Roles and responsibilities

Cybersecurity is an organisation-wide concern. It begins with end-users and extends to the board room. It is important that all stakeholders understand the risks associated with cyber threats and be aware of the common threat vectors.

It has been recognised that adopting the right behaviour in the business environment is a first and major step towards mitigating cyber-related risks.

4. Threat vectors

A threat vector can be defined as a path or a means by which a cybercriminal (often called hacker) can gain access to systems.

The access can be obtained through several point of entries into systems. Cybercriminals will exploit these vulnerabilities (i.e., the attack surface).

Below is a list of common threat vectors, for which Terra has implemented security measures to prevent or mitigate cyber-related risks:

- Network (The perimeter and the local corporate network infrastructure)
- End-users (Employees are often the main target of cybercriminals who use social engineering/ networking to gain sensitive information which then used to access systems or trick end-users to open a gateway to infiltrate systems)
- E-mail (Common phishing attacks, scams, spoofing of identity, and malicious attachments).
- Application (Specifically web-based applications are at risk of attacks through Structures Query Language (SQL) injections and cross-site scripting).
- Remote Access (A corporate device using an unsecured wireless hotspot can be compromised).
- Mobile devices (Smart phones, tablets, and other mobile devices can be used as devices to infect a corporate network and/or steal sensitive data).

5. Overview of security measures

Terra has adopted a proactive approach in respect to cyber security and has implemented security measures with the objective of safeguarding its IT assets. The main measures are described below:

- End-users abide by an internal IT Usage Policy / Electronic Code of Conduct, which describes the usage of Information Technology within the business organisation.
- Secured physical infrastructure (Data Centers).
- Access control and locked Data Centers located within office with 24/7 alarm monitoring and security officers at parameter.
- Physically and virtually segmented network infrastructure through centralised next-generation firewalls and switches with defined controlled zones and policies.
- Fixed IP addresses are assigned to end-users by the Group IT Department on the corporate wired network , thus allowing end-users' identification and the application of access policies.
- Dynamic IP addresses are pre-defined for guest users by the Group IT Department on the corporate wireless network with limited access to the Internet only.
- All Internet connections on the network infrastructure are firewalled, controlled through firewall policies and monitored.
- Controlled software/applications. End-users cannot install software or applications on their workstations and/or laptops. All applications are validated and installed by authorised IT personnel. This also ensures legal usage of software packages.
- Centralised update servers to download and deploy latest security patches and updates to all endpoints (remote computing devices, including desktops and laptops).
- Advanced Threat Protection (ATP). Automated and Artificial Intelligence (AI)-driven software agents installed on all endpoints to protect against known, unknown (zero-day) and targeted threats.
- Encryption of email facility provided to key personnel who require an additional level of security when sending sensitive data over the Internet.
- Physically segregated and controlled Wi-Fi network to avoid potential data leakage and theft.

6. Technologies implemented

Terra has deployed a number of technologies to protect its network infrastructure and mitigate cyber-related risks. The main technologies are described below:

Next-generation firewalls, which allow:

- Secured and controlled access to the external world (Internet)
- Identification and control of applications on the traffic flow.
- Physical segmentation of network and intra and inter zones traffic.
- Application-level policies set up on the firewall.
- Subscription to updated threat prevention database (known threats).

- Subscription to updated threat prevention database (known threats).
- Subscription to cloud-based analysis of uncategorised threats (unknown threats).
- Subscription to web content filtering database (ULR filtering).
- Threat monitoring, notification and isolation.
- DoS protection against volumetric Internet attacks.

Cloud-based email security gateway to handle inbound and outbound emails, which allows:

- Redundant MX protocol for fail-over purposes.
- Content filtering of all email and attachments.
- Antivirus scanning of emails.
- Automatic quarantine suspicious emails and notification to recipients.
- Subscription to a blacklist database to immediately drop suspicious emails and spam-type emails.
- DoS protection against volumetric email attacks.

Next-generation endpoint protection platform, which allows:

- Real-time detection and prevention of known threats using static AI.
- Real-time detection and prevention of unknown threats using behavioural AI.
- Embedded AI threat intelligence and threat indicators.
- Recovery with remediation and rollback features.
- Device control for USB and Bluetooth peripherals
- Complete visibility through dashboard and reporting of threats.
- Rogue device discovery and application inventory.

Administrative privileges on each endpoint, which allows:

- Control of applications and software packages installed on endpoints.
- Ensure compliance with end-user software agreement.
- Genuine software installation and licenses control.

Centralised patching and updates deployment, which allows:

- Automated download of latest patches and updates for endpoints.
- Deployment of approved patches and updates to all endpoints.
- Fast deployment of patches to all endpoints.
- Centrally-managed rollback facility for updates/patches.

On-demand encryption of sensitive emails, which prevents:

- Potential eavesdropping and data theft.

WiFi access points at selected areas for end-user and guest users, which are:

- Password protected.
- Physically and virtually isolated to the enterprise network.
- IP addressing is independently handled by the WiFi administration platform.
- Internet access is controlled and filtered by firewall.

Awareness about latest cybersecurity threats and risks, through:

- Communication by email to end-users about virus and malware outbreaks.
- Communication by email to end-users about scam and phishing attempts.
- Behaviours to adopt when there is a scam or social engineering attempt.

A defined backup and disaster recovery policy, which allows:

- A mix of on-site and off-site backups.
- A mix of full and incremental backups.
- Capacity to perform a full recovery of an impacted system.
- Capacity to perform a granular recovery of an impacted system.
- Retention of data allowing specific recovery dates within a set period.