TERRA MAURICIA LTD

Information Technology Security Policy (Version 2017 - V1.1)

For the future. From 1838

terra

Information Technology security 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 endpoints).

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 have been relying on information technology to conduct their business operations. The advent of the Internet as a communication medium with the external world has become essential yet it has open up new opportunities for cybercriminals.

Indeed, organisations are increasingly being the target of cybercriminals whose actions can lead to loss of business and reputational damage particularly if adequate security measures are not in place.

This situation has prompted organisations to address risks related to cyber threats and security breaches. Terra has always adopted a prudent approach in terms of cyber security. Numerous technologies and measures have been implemented to protect the organisation from cyber threats. Investment in the cybersecurity field has been a recurring budget item since many years.

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 security technologies and measures are purposely "transparent" to end-users.

Moreover, the Group IT Department strives to communicate with end-users when a threat is found in the "wild" and also remind of behaviours to adopt when facing a potential threat.

Please note that 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.

terra

4. Threat vectors

This is a list of threat vectors for which actions have been taken to prevent or mitigate cyberrelated risks:

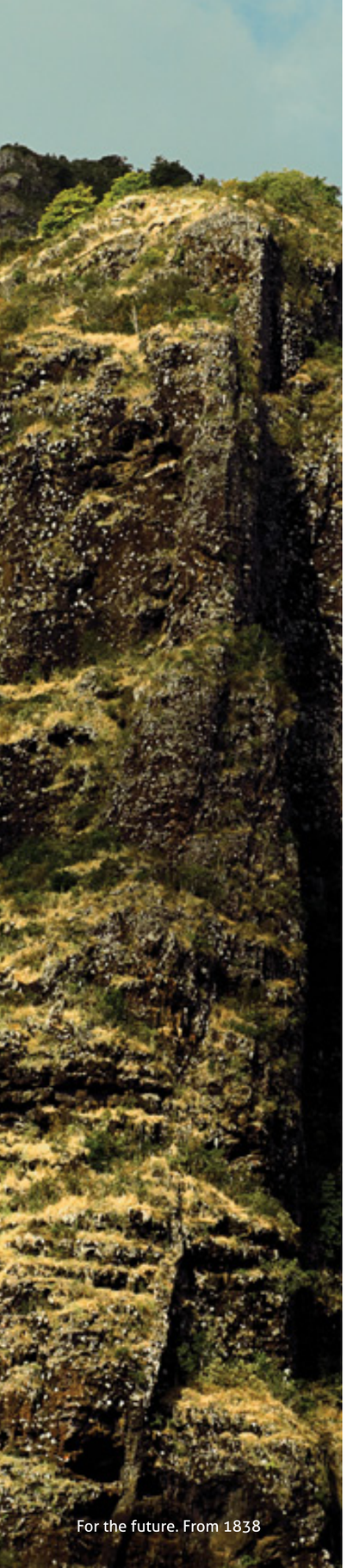
- Malicious files and applications such as virus and malware. (Web-browsing, E-mail, Software, Download).
- Scams, phishing and spoofing of user identity (E-mail)
- Vulnerability exploit (O/S, Web-browsing, E-mail).
- Unauthorised access rights and privileges (Access control).
- Denial of Service (Network attacks at the Internet gateway).

5. Overview of security measures

Terra has adopted a prudent approach in respect to cyber security and has implemented practices with the objective to safeguard the IT assets. The main measures are described below:

- Secured physical infrastructure.
- Access control and locked server rooms with 24/7 alarm monitoring and security officers at parameter.
- Physically segmented network infrastructure through centralised next generation firewalls with defined controlled zones and policies.
- IP addresses are assigned by Group IT function, thus allowing end-users' identification.
- No DHCP (Dynamic Host Control Protocol) on the enterprise network to prevent unauthorised access or rogue connections to the enterprise systems.
- A zero back-door policy is enforced. All Internet connections on the network infrastructure are firewalled, controlled and monitored.
- End-users abide to an internal IT Usage policy and Code of Conduct, which describe the usage of systems within the business organisation.
- Controlled applications. End-users cannot install software or applications on their workstations and/or laptops. All applications are controlled and installed by authorised IT staff. This also ensures legal usage of software packages.
- Centralised update servers to download and deploy latest security patches and updates to all end-points.
- Physically segregated and controlled Wi-Fi network to avoid potential data leakage and theft.

terra



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:

Centralised next-generation firewalls, which allow:

- Secured and controlled access to the outside world (Internet)
- Identification of applications on the traffic flow.
- Physical segmentation of network and intra and inter zones traffic.
- Application defined policies set up on the Firewall.
- Subscription to 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.

Email appliances at gateway to handle inbound and outbound emails, which allow:

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

Centralised antivirus with administration platform, which allows:

- Automated download of latest virus signatures and antivirus engines.
- Automated deployment of virus signature databases to each end-point.
- Incoming emails controlled by anti-virus at the gateway.
- Scheduled scanning of all end-points.
- Online scanning when application is launched on end-points.
- Monitoring of virus and malware identification on network.

Administrator privilege on each end-point, which allows:

- Control of applications and software packages installed on workstations/laptops.
- Ensure compliance to 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 end-points.
- Automated deployment of approved patches and updates to all end-points.
- Fast deployment of patches to all end-points.

Encryption of internal traffic between remote sites, which prevents:

- Intra-network eavesdropping and data theft.
- Intra-network data and traffic control.

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

- Password protected.
- Physically isolated to the enterprise network.
- IP addressing is independently handled by the WiFi Access Point.
- 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:

- Full recovery of an impacted system in case of cyber-related issues.
- Granular recovery of centralised backup data (e.g. specific files).
- Retention of data allowing specific recovery dates within the retention period.

- o - o - o - o -