TERRA MAURICIA LTD

Information Technology Policy
(Version 2023 - V1.3)

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

In today's rapidly digitising world, organisations are increasingly intertwined with Information Technology (IT) as a hub of their business operations. The Internet, the connection of global communication and commerce, has seamlessly integrated with contemporary business models, unlocking unprecedented avenues of growth and innovation. Yet, this digital evolution brings inherent vulnerabilities, offering fertile ground for nefarious actors seeking to exploit these technological dependencies.

Recent trends underscore a troubling escalation in cyberattacks targeting organisations. These malevolent activities, facilitated by progressively advanced tools, have grown in their complexity and potential for damage, ranging from reputational degradation to crippling business interruptions. The cyber risks are profound, especially in Mauritius, with its visionary stride towards establishing itself as an IT epicentre in the region. Beyond the technical challenges, it's imperative to consider the legal landscape. Under the Mauritian Data Protection Act, organisations are legally mandated to safeguard personal data, elevating cybersecurity from merely an IT challenge to a binding legal obligation.

Recognising the evolving threat landscape, Terra has been at the forefront of adopting a proactive approach to cybersecurity. Our strategy is evident in our selection of leading-edge security technologies. In our commitment to fortifying our cyber defences:

- We've integrated **Darktrace's** Enterprise Immune System, leveraging machine learning and AI algorithms to detect, respond to, and mitigate internal and external threats in real time.
- **SentinelOne's** endpoint security solution has been deployed, providing a multi-layered defence mechanism against known and zero-day threats while offering advanced threat hunting and automated response capabilities.
- For our communication infrastructure, **Mimecast's** advanced email security solutions have been implemented, ensuring robust protection against phishing, spear-phishing, and other advanced email-based threats.

Such decisive investments underscore Terra's unwavering dedication to safeguarding IT assets and data, implementing numerous protective mechanisms, and guarding our organisation against cyber threats.

The essence of this document is twofold:

1. To elucidate the current cyber threat milieu, highlighting its implications for the business landscape in Mauritius and on the global stage.

2. To provide a comprehensive overview of the security protocols, technological solutions, and protective measures, Terra has strategically instated to secure its invaluable IT assets.

It's pivotal to underline the designed subtlety of our IT security framework, operating unobtrusively, ensuring an uninterrupted experience for end-users. Concurrently, Terra's IT Department remains vigilant and agile, consistently updating itself on emerging cyber threats. Timely communication with our user base remains a priority, ensuring they are apprised of the latest threats and are equipped with knowledge on the best course of action in potential threat scenarios.

3. Roles and responsibilities

Cybersecurity is not confined to just one department or set of hands; it envelops the entire organisation. From individual end-users to the leadership in the boardroom, everyone plays a pivotal role in safeguarding our digital assets. Recognising and understanding cyber risks and being aware of common threat vectors is a shared responsibility across all levels of the organisation.

The IT Manager and Group IT Manager are accountable for overseeing the organisation's cybersecurity posture. This involves:

- Setting the strategic direction for cybersecurity initiatives.
- Allocating resources, both financial and human, to cybersecurity endeavours.
- Receiving and reviewing periodic security updates and threat assessments.

IT Department: Charged with the technical implementation and management of security measures. Their duties encompass:

- Deploying, monitoring, and maintaining security tools and solutions.
- Conducting periodic security assessments and vulnerability scans.
- Ensuring regular updates and patches are applied to all systems.
- Coordinating and executing incident response plans in the event of a security breach.

End Users: Every employee, irrespective of their role, is a critical player in our cybersecurity framework. Their responsibilities include:

- Adhering to the IT Usage Policy and any other related guidelines.
- Reporting any suspicious activities or potential security breaches to the IT department.
- Regularly updating and securing their passwords.
- Participating in cybersecurity awareness training sessions.

While Terra has made significant investments in state-of-the-art cybersecurity tools and technologies, it's essential to acknowledge that the end-user often remains the most susceptible link in the security chain. Technology can shield us from a multitude of threats, but human behaviour is harder to predict and control. This underscores the imperative nature of fostering a culture of cybersecurity awareness and vigilance among all employees. A well-informed and cautious end-user can often be the first and most effective line of defence against potential cyber threats.

4. Threat vectors

At the heart of cybersecurity lies the understanding of threat vectors—these are pathways or means through which cybercriminals can infiltrate or compromise systems. The point of entry they select often depends on the vulnerabilities (or the attack surface) they identify within an organisation's infrastructure or its people.

Terra has instituted a robust set of security measures to address the diverse and evolving threat vectors. Here's a closer look at the common vectors and Terra's approach to managing them:

4.1. Network Infrastructure: The boundaries of our corporate network, both external perimeters and internal segments, are primary targets. Measures include:

- Advanced firewall protections.
- Intrusion detection and prevention systems.
- Rigorous network monitoring.

4.2. End-users: Arguably the most unpredictable vector, employees can unwittingly provide cybercriminals access. Threats often manifest as:

- Social engineering attacks aim to extract sensitive information.
- Manipulative tactics are designed to trick users into compromising security. Recognising the vulnerability of this vector, Terra emphasises regular cybersecurity training and awareness campaigns for its staff.

4.3. Email: A common attack conduit due to its ubiquitous use. Threats encompass:

- Phishing or spear-phishing attempts.
- Identity spoofing.
- Malicious attachments or links. Terra employs advanced email filtering and monitoring systems to combat these, including solutions like Mimecast.

4.4. Applications: Our reliance on web-based applications exposes us to specific threats such as:

- SQL injections targeting databases.
- We partner with trusted SaaS solution providers to ensure the highest standards of data security. Each year, our cloud SaaS solutions—including MDA, Oracle Apex, Office 365, and FIS—are audited to check compliance with product contracts.

4.5. Remote Access: Devices connecting remotely to corporate resources are potentially vulnerable, especially on unsecured networks. However, Terra has deployed Mimecast Web Security for those working remotely on laptops. As a web security gateway, Mimecast inspects web requests and filters URLs using its advanced threat intelligence and security analytics. By aligning with Terra's acceptable use controls, security policies, and bypass exceptions, it determines the safety and appropriateness of a website. This combined approach of rigorous remote access guidelines, VPN solutions, and Mimecast Web Security guarantees a fortified communication pathway, significantly reducing associated risks.

4.7. Cloud and Third-Party Services: This vector is becoming more prominent with the increasing adoption of cloud solutions and third-party services. Misconfigurations or vulnerabilities within these services can expose Terra to risks. Regular audits, access controls, and partnerships with reputable providers mitigate these threats. Terra also complies with the Data Protection Act (2017) in this regard.

4.8. Industrial IoT in Manufacturing: While our SCADA systems in manufacturing operate within a closed network ring, ensuring they don't pose a direct threat to our primary network, it's vital to monitor and secure them against potential attacks targeting industrial systems.

While Terra takes pride in its proactive approach, integrating leading technologies and best practices, it must be understood that cybersecurity is continually evolving. Our commitment is to protect against known threats and stay vigilant against emerging ones.

5. Overview of security measures

In the face of a perpetually evolving cyber threat landscape, Terra remains steadfast in its commitment to cybersecurity. We have diligently architected a multi-layered security framework to safeguard our vital IT assets. Below are the primary measures we've implemented:

- **IT Usage Policy & Electronic Code of Conduct:** All end-users adhere to our comprehensive policy stipulating the appropriate and secure use of Information Technology resources within the organisation. This policy serves as a foundation for ensuring user accountability and awareness.
- **Secured Physical Infrastructure:** Our Data Centers are fortified with rigorous security protocols, including 24/7 alarm monitoring, security personnel patrolling the perimeter, and stringent access controls ensuring only authorised personnel can enter.
- **Network Segmentation:** Our network infrastructure, both physical and virtual, is securely segmented using centralised next-generation firewalls and switches. Defined zones and policies ensure controlled and monitored inter-segment communications.
- **IP Address Management:** We assign fixed IP addresses to end-users on our corporate wired network, facilitating user identification and the seamless application of access policies. Guest users on our wireless network are assigned dynamic IP addresses, restricting their access only to the Internet.
- **Internet Connection Security:** All internet connections are shielded by firewalls, with traffic governed by well-defined firewall policies. This continuous monitoring ensures any suspicious activity is swiftly detected and addressed.
- **Software and Application Control:** To fortify our defences against potential threats, we restrict end-users from adding unauthorised software or applications to their devices. The IT department takes the lead in vetting, approving, and installing all applications, ensuring a blend of optimal security and adherence to licensing terms.
- **Patch Management:** Our centralised servers ensure the timely downloading and deploying of the latest security patches and updates to all endpoints, maintaining the security integrity of our devices.
- **Advanced Threat Protection (ATP):** We leverage AI-driven software agents across all endpoints, offering protection against a broad spectrum of threats, from well-documented to emerging zero-day vulnerabilities.
- **Email Encryption:** Recognising the sensitivity of certain communications, we offer email encryption to key personnel. This added layer ensures the security of sensitive data when transmitted over the Internet.
- **Wi-Fi Network Security:** Our Wi-Fi networks are designed with security in mind. Physical segregation and stringent controls prevent unauthorised access and potential data leakage.
- **Multi-Factor Authentication (MFA):** We've implemented MFA across critical systems to bolster access security. This ensures that user identity is verified through multiple methods before granting access.
- **Security Awareness Training:** Employees undergo security training programs at regular intervals. These sessions equip them with the latest knowledge about cyber threats and best practices to counteract them.

- **Principle of Least Privilege:** In line with this principle, team members receive only the access and privileges essential for their specific roles, safeguarding the more vulnerable segments of our IT infrastructure.
- **VPN for Remote Access:** Recognising the vulnerabilities arising from remote access, we've established VPNs, guaranteeing that remote connections to our systems remain secure and encrypted.

Our collective security measures underscore Terra's unwavering dedication to creating and maintaining a cyber-resilient environment. As the threat landscape evolves, so will our strategies, ensuring we remain a step ahead and uncompromised.

6. Technologies implemented

Terra's commitment to cyber resilience is underpinned by its deployment of a myriad of state-of-the-art technologies to protect network infrastructure and mitigate cyber-related risks. Here's a breakdown of the core technologies and systems in place:

1. Next-Generation Firewalls:

- Secured and controlled access to external interfaces (Internet).
- Traffic flow application identification and control.
- Physical and virtual segmentation of network traffic, both intra and inter-zone.
- Application-specific firewall policies.
- Subscriptions to updated threat prevention databases and cloud-based analysis for uncategorised threats.
- Web content filtering through URL filtering databases.
- Advanced threat monitoring, notification, and isolation.
- Denial of Service (DoS) protection against substantial Internet-based attacks.

2. Cloud-based Email Security:

- Redundant MX protocol implementation for fail-over scenarios.
- Filtering for email content and attachments.
- Antivirus scanning capabilities for emails.
- Suspicious emails are quarantined automatically, with notifications sent to recipients.
- Blacklist database integration to counter suspicious emails and spam.
- DoS protection against massive email attacks.
- Integration with Mimecast for enhanced email protection and Office 365 as the primary mail service.

3. Endpoint Security:

- Real-time detection of known threats leveraging static AI and unknown threats through behavioural AI facilitated by the next-generation endpoint protection platform.
- Embedded AI for threat intelligence and indicators.
- Recovery mechanisms with remediation and rollback features.
- Control measures for USB and Bluetooth device connections.
- Comprehensive visibility via threat reporting dashboards.
- Discovery tools for rogue devices and application inventories.

4. Administrative and Application Controls:

- Strict administrative privileges on each endpoint.
- Standardised and legal software installations ensured.
- Automated centralised patch management, with the capability for quick deployment and rollback.

5. Email Encryption: Encryption tools are available on-demand to prevent potential eavesdropping and unauthorised data access.

6. Wi-Fi Networks:

- Password-protected access points are provided by Ruckus and Aruba.
- Physical and virtual segregation from the primary enterprise network.
- Independent IP address management via the Wi-Fi administration platform.
- Firewall-regulated and filtered Internet access.

7. Cybersecurity Awareness:

- Periodic email communications about emerging threats, scams, and best practices.

8. Backup and Recovery:

- Comprehensive backup strategies involving on-site and off-site backups.
- Capabilities for full system recovery and granular data restoration.
- Data retention policies ensure recovery from specific points in time.

9. Darktrace Enterprise Immune System: Providing continuous monitoring and real-time threat detection using AI and machine learning algorithms.

10. Zero Trust Security via RADIUS Server: Serving as a cornerstone for validating VPN accesses and wireless connections to corporate networks, specifically for the 'gold' and 'premium' categories.

11. Web Security with Mimecast: Ensuring endpoint protection for devices operated from remote locations or home environments.

12. Digital Signature with DocuSign: Facilitating secure and verified digital signatures for online transactions and documentation.

13. Intrusion Detection and Prevention Systems (IDPS): Constantly monitoring network traffic patterns and promptly identifying malicious activities.

14. Security Information and Event Management (SIEM) systems: Providing real-time analysis of security alerts generated by applications and network hardware.

15. Secure Access Service Edge (SASE): Combining network security with wide area networking capabilities within a unified cloud service, enhancing safety for remote users and cloud applications.