TERRA MAURICIA LTD

Information Technology Usage Policy

(Version 2023 - V2.4)

For the future. From 1838

Governing the use of computers, computer services, and communication devices, including email and Internet

Table of Contents

1. Introduction

The Information Technology (IT) Usage Policy (the "Policy") is a comprehensive guide for employees on the appropriate and secure use of Terra Mauricia Ltd and its subsidiaries (collectively referred to as the "Group") information systems and services. This Policy aims to protect the company's assets, data, and reputation while promoting efficient and responsible utilization of these resources. By adhering to the guidelines and best practices outlined in the Policy, employees contribute to maintaining a secure, compliant, and productive IT environment for the entire organisation. The Policy should be read in conjunction with other code of conducts, procedures, manuals, ethical code of conduct already implemented within the Group.

1.1. Scope

This Policy applies to all employees, contractors, and third parties who use or access the Group's information systems and services, including computer hardware, software, applications, data, electronic files, communication devices, and networks.

1.2. Policy Compliance

Compliance with this Policy is mandatory. Violating this Policy may result in disciplinary actions, including termination of employment. The Group may also pursue legal remedies if necessary.

1.3. Policy Review and Updates

This Policy may be revised periodically to adapt to technological advances, legal requirements, or other changes. Employees will be informed of any updates or changes to this Policy. Each employee is responsible for staying informed and adhering to the most current version of the Policy.

2. Roles and Responsibilities

Each member within the Terra ecosystem plays a unique and vital role in ensuring our digital environment remains secure.

- **Policy Custodian:** This role ensures the policy stays up-to-date and aligns with Terra's governance strategy.
- **Cluster IT Manager:** A pivotal role focused on managing IT and security risks across Terra's entities.
- **Users:** A diverse group encompassing employees, trainees, partners, and more. Their duty is to understand, adhere to, and actively safeguard Terra's IT assets.

3. Information Security

Ensuring the confidentiality, integrity, and availability of our data is of paramount importance. All employees, contractors, and stakeholders are required to understand and adhere to our data classification and handling procedures.

3.1. Data Protection and Privacy

The Group is committed to complying with the Data Protection Act (2017) and ensuring personal data's lawful collection, processing, and storage. Employees who manage or have access to personal data must adhere to the principles outlined in the Act, including obtaining proper consent and maintaining accurate records of processing operations.

3.2. Copyright and Intellectual Property

Employees must respect the intellectual property rights of others, including copyrights, trademarks, and patents. Unauthorised copying or distribution of third-party materials, including software and digital media, is strictly prohibited and may result in legal action against the Group and the employee.

3.3. Confidentiality and Encryption

When sending confidential information via email or other electronic means, employees should use encryption to ensure the security and privacy of the data. The Group IT Department can assist with encryption tools and best practices.

3.4. Monitoring and Access

The Group reserves the right to monitor and access any data or electronic files stored on its systems, including emails and other communications. This monitoring may be conducted without the employee's permission and can include files on computers, servers, storage appliances, cloud services, and communication devices.

3.5. Incident Reporting and Response

Employees should promptly report any security incidents to the Group IT Department, such as data breaches or unauthorised access. The Group is committed to investigating and addressing any security incidents to protect its information systems and the personal data of its employees and customers.

3.6. Advanced Threat Detection with Darktrace

- **Adoption of Darktrace:** The Group has onboarded Darktrace as a strategic initiative to fortify our cybersecurity stance. Darktrace employs artificial intelligence to incessantly scrutinize our IT traffic, pinpointing and impeding abnormal patterns or security threats in real-time. This includes, but is not limited to, incidents involving ransomware, malware, and suspicious links.
- **Continual Monitoring:** Darktrace ensures that our IT environment is under constant surveillance. All employees should comprehend that any deviations from the norm or suspicious activities within the network, such as malware downloads or access to dubious links, will set off alerts, warranting scrutiny from the IT department.
- **Immediate Response:** Any alerts or potential security concerns flagged by Darktrace will instigate immediate actions. Our proactive stance ensures threats are swiftly identified, isolated, and rectified to safeguard our digital assets.

3.7. Two-Factor Authentication with Radius Server

- **Enhanced Authentication:** To ensure only authorized individuals gain access to our IT resources, we have implemented a RADIUS server to act as a two-way authentication mechanism. This process remains largely seamless to users, enhancing security without adding undue complexity.
- **VPN & Wireless Access Criteria:** Access to VPN and wireless services will only be granted under the following conditions:
  - o Validation of the user's credentials.
  - o Verification that the computing device being used is registered within our Domain Controller.
  - o Confirmation that the user's machine has a valid root certificate installed.

3.8. Role-Based Access Control (RBAC)

- **Definition and Purpose:** RBAC ensures that access to IT resources and data is based on roles within the Group. Under this system, employees have access only to the IT resources they need to perform their specific job functions, ensuring that sensitive data is only accessible to those with the appropriate permissions.
- **Implementation:** The Group IT Department will define and manage roles, ensuring that access permissions are appropriately assigned and modified as roles change within the organization. Regular audits will be conducted to ensure compliance with RBAC principles and to identify any unnecessary permissions that may be revoked.

3.9. Password management policy

The security of our systems hinges significantly on robust password practices. This policy provides directives to ensure passwords are managed securely and consistently across all levels of access: user-level, system-level, and service accounts.

Guidelines:

1. **Prohibited Passwords:** Blank or easily guessable passwords such as "password", "12345", "qwerty", or "pass1234" are strictly forbidden, regardless of the significance of the account. Moreover, passwords should never be basic dictionary words or easily associated with the user (like birthdays or anniversaries).
2. **Complexity Requirements:** All passwords must adhere to the following criteria:
   - o Minimum length of eight characters.
   - o A combination of both uppercase and lowercase letters.
   - o At least one numeric digit.
   - o At least one special character (e.g., !, @, #, $, %, ^, &, *).
3. **Unique Passwords:** It is crucial to ensure that passwords are unique to each system. Replicating passwords across multiple systems amplifies the risk in case one system gets compromised.
4. **Avoid Personal Platform Passwords:** Never use passwords that you've set up for personal platforms or services, such as Facebook, Instagram, or any other social media. This practice ensures a breach in one platform doesn't render your professional accounts vulnerable.
5. **Change Regularly:** Passwords must be updated at regular intervals for optimum security. By standard protocol, you will receive a prompt to change your password every 90 days. Should you have any concerns or suspicions about a system breach or compromise, it's imperative to modify your password immediately. Be advised that certain systems have in-built periodic change reminders, which are in alignment with this policy's objective to maintain secure credentials.
6. **Store Safely:** Never write down passwords or store them in unsecured locations. If you need to document them, use a secure, encrypted password manager.

4. Multi-Factor Authentication (MFA) Requirements

To further enhance the security of our systems and data, the Group has implemented Multi-Factor Authentication (MFA) across various applications and services. MFA requires users to provide multiple forms of identification before gaining access, significantly reducing the risk of unauthorized access.

Application of MFA:

1. **Office 365 Mail Access:** In addition to a password, accessing your O365 mail will prompt for a secondary authentication via your registered mobile phone number. This might be in the form of a text message, a call, or an app notification, depending on the settings chosen.

2. **Authenticator Apps:** For certain services, Terra Group employs authenticator apps which generate time-sensitive codes for authentication. Users must install the specified authenticator app on their mobile devices and link it to the respective service. Each time access is sought, the app will produce a unique code that must be entered, along with the regular password.

User Responsibilities:

- **Updated Information:** It is vital to keep personal details, especially mobile phone numbers and authenticator app linkage, updated in the system. Outdated information can impede access.

- **Prompt Response:** Users should swiftly respond to MFA prompts. Unexpected MFA requests, especially unsolicited ones, should be immediately reported to the IT department as they might indicate unauthorized access attempts.

- **Device Security:** If MFA utilizes personal devices, such as smartphones, they should be secured with reliable lock methods – PIN, password, fingerprint, or face recognition. This precaution ensures another security layer if the device gets misplaced or stolen.

5. Asset Management

Safeguarding our IT assets is critical. Proper management ensures we can track, utilize, and dispose of assets securely.

5.1. Inventory

Purpose: To account for and monitor all IT assets throughout their life cycle.

- **Scope:** Includes all IT-related hardware (e.g., laptops, servers), software licenses, and other related assets.

- **Responsibility:** The IT Department is tasked with updating and auditing the inventory regularly.

- **Action:** All new acquisitions must be reported to IT for inventory logging. Periodic audits will ensure the accuracy and completeness of the inventory list.

5.2. Physical Security

Purpose: To ensure sensitive data and systems are shielded from unauthorized access.

- **Scope:** This covers areas like server rooms, data centers, and other locations housing sensitive equipment or data.

- **Responsibility:** Security teams or appointed personnel will manage access controls.

- **Action:** Employees must display proper identification when entering these zones. Visitors require prior approval and must always be accompanied by authorized staff. Security breaches or suspicious activity should be reported immediately.

5.3. Acceptable Use

Purpose: To ensure IT assets are used effectively, securely, and ethically to serve the organization's best interests.

- **Scope:** This policy encompasses all IT assets provided by the organization, including but not limited to computers, mobile devices, software, networks, and peripherals.
- Guidelines:
  - **Business Purposes:** IT assets are primarily for business-related activities. Incidental personal use is permissible, provided it does not interfere with work responsibilities, breach security protocols, or involve inappropriate content.
  - **Care and Maintenance:** Users should handle IT assets with care to prevent damage, theft, or loss. This includes not leaving devices unattended in public areas, and refraining from installing unapproved software that might harm the device or network.
  - **Security:** Users should not bypass security protocols or install unauthorized software. Regularly update passwords and ensure that devices are locked when unattended.
  - **Ethical Use:** Users should refrain from using IT assets for activities that may be considered unethical, illegal, or damaging to the organization's reputation. This includes, but is not limited to, viewing, or sharing inappropriate content, cyberbullying, or engaging in fraudulent activities.
  - **Resource Consumption:** Be considerate about resource usage. Refrain from activities that unnecessarily consume bandwidth or storage, such as streaming non-work related videos during business hours or storing large personal files on company servers.
- **Consequences:** Failure to adhere to the acceptable use policy can lead to disciplinary actions, ranging from warnings to revocation of IT privileges or further legal actions, depending on the severity of the breach.

5.4. Software and Applications

Employees may only install software or applications on the Group's systems with prior approval from the Group IT Department. Unauthorised installation or copying of software may lead to legal issues, system incompatibility, or exposure to viruses and other security risks.

5.5. Media Disposal

To prevent unauthorized access or data leakage from discarded or obsolete electronic media, including but not limited to all forms of electronic storage, hard drives, flash drives, CDs, IT personnel will oversee and perform the disposal process of such electronic media. All Media must undergo a secure erasure process. If the device is no longer functional or data cannot be securely wiped, it should be physically destroyed. Receipts or documentation for secure disposal or destruction should be retained.

5.6. Reporting Lost or Stolen

In the unfortunate event that IT assets go missing, a swift response is crucial to safeguarding the organization's information. Here's what employees need to do:

Immediate Reporting: Report any lost or stolen IT assets, such as laptops or mobile devices, promptly to both your supervisor and the Group IT Department and to the Data Protection Officer of the employee's company. This ensures that appropriate security responses, including remote wipe capabilities, can be initiated without delay.

Remote Wipe Abilities:

The Group IT Department may remotely wipe data from lost or stolen devices, ensuring that confidential and sensitive data is protected. Once a device is reported missing, the IT team will evaluate the situation and may initiate a remote wipe to prevent unauthorized access to company data.

Device Recovery: If a device is recovered after a remote wipe, consult with the IT Department. The device will require a thorough check and possible reconfiguration before being deemed safe for use again.

It is in everyone's best interest to ensure the immediate reporting of such incidents. Quick action minimizes potential risks and helps to protect both the individual and the organization.

6. BYOD (Bring Your Own Device) Policy

At Terra Group, we recognize the convenience and productivity benefits of allowing employees to use their personal devices for work-related tasks. However, to protect our information assets and ensure a secure IT environment, certain requirements and guidelines must be met:

6.1. Supported Devices and Enrolment

- **Device Types:** Smartphones, tablets, and iPads are the accepted personal devices for BYOD purposes.
- **Enrolment Process:** Before using personal devices for work, users must:
  1. Formally request access.
  2. Present their devices to their respective IT departments for enrolment and verification.
- **Permissible Access:** Once enrolled, employees can use their personal devices to access public company resources like emails, calendars, and contacts. However, BYOD devices will connect through a separate network, ensuring internal networks remain inaccessible for security reasons.

6.2. Risks, Liabilities, and Protections

- **Employee Liability:** Employees understand and accept the risks tied to BYOD practices. This includes potential loss of both personal and company data due to various factors such as system crashes, software/hardware issues, malware, or other unexpected errors. The responsibility for these risks primarily rests with the employee.
- **Antivirus Measures:** To maintain security:
  1. The Group may install its chosen antivirus software on an employee's device.
  2. Alternatively, employees might be instructed to install specific antivirus software, monitored, and verified by the IT department.
  3. The IT department will conduct periodic checks on these devices to ensure consistent security standards.
- **Protection Rights:** If a BYOD device poses any perceived threat to the company's information assets, the Group retains the right to:
  1. Disconnect the device.
  2. Disable certain services without prior notification.
  3. Remotely wipe any company-related data from the device.

This BYOD policy aims to strike a balance between flexibility and security, ensuring that the Group's IT infrastructure remains robust and secure while providing employees with the convenience of using their personal devices.

7. Ethical and Efficient Use of AI Technologies

7.1 Ethical Consideration

Employees leveraging AI tools should always weigh the ethical implications of their actions. It's pivotal to use AI to augment decision-making, rather than to introduce bias or discriminatory practices.

7.2 Transparency with AI

For scenarios where AI interacts with customers, it is crucial to maintain transparency. Customers deserve to know when they're communicating with, or receiving information from, an AI system.

7.3 Limitations of AI

Recognize and respect the limitations intrinsic to AI systems such as ChatGPT. These tools derive their knowledge from the data they have been trained on and might not always provide entirely accurate or context-aware responses.

7.4 Data Privacy with AI

Safeguarding data remains paramount, especially when engaging with AI platforms. Even though systems like ChatGPT are designed not to retain personal chat data, always approach these platforms with a privacy-first mindset.

7.5 AI and ChatGPT Risk Awareness:

Understand that while AI technologies, including systems like ChatGPT, offer myriad advantages, they are not without their vulnerabilities. Refrain from divulging sensitive or classified information to AI-driven chatbots and platforms.

8. Network and Internet Usage

8.1. Responsible Use

Employees must use the Group's network and internet resources responsibly and professionally. The primary purpose of these resources is for business-related activities, and personal use should be limited and not interfere with work responsibilities.

8.2. Prohibited Activities

Using the Group's network and internet resources for illegal, unethical, or offensive activities, including accessing or distributing pornographic materials, harassment, or engaging in activities that could damage the Group's reputation, is strictly prohibited.

8.3. Internet Access Restrictions

The Group reserves the right to restrict access to internet resources deemed non-work related, offensive, or bandwidth intensive. Employees should only attempt to bypass these restrictions or download unauthorised software with permission from the Group IT Department.

8.3.1 Internet

Employees must use the Group's email and internet services responsibly, considering the security risks and potential impact on the Group's reputation. Confidential information should be encrypted with a password when sent via email. Employees should seek advice from the Group IT Department when in doubt about sending large attachments or using specific keywords.

Use of the Internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of the Company in mind. Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring the Company into disrepute, create or transmit material that might be defamatory or incur liability on the part of the Company, or adversely impact on the image of the Company.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the Company's computer network.
- Personal use of the internet must not cause an increase in significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- Users must not "hack into" unauthorised areas.
- Users must not download commercial software or any copyrighted materials belonging to third parties unless such downloads are covered or permitted under a commercial agreement or other such licence.
- Users must not use the internet for personal financial gain.
- Users must not use the internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the internet to send offensive or harassing material to other users.
- Use of the internet for personal reasons (e.g., online banking, shopping, information surfing) must be limited, reasonable and done only during non-work time such as lunchtime.
- Staff may face disciplinary action or other sanctions (see below) if they breach this policy and/or bring embarrassment to the Company or bring it into disrepute.

8.4. Security Precautions

Employees must be cautious when using the Internet to avoid inadvertently introducing security threats to the Group's systems, such as malware or viruses. Only download software or open attachments from unknown sources with approval from the Group IT Department. Additionally, only provide network access to third parties with proper authorisation.

9. Email and Communication

Emails and electronic communications are essential tools for our organization. When used effectively, they facilitate collaboration, streamline workflows, and ensure transparency. However, when misused, they can lead to security breaches, miscommunication, and potential reputation damage. As such, employees are expected to adhere to the following guidelines:

9.1. General Usage

- **Professionalism:** Use emails and electronic communications responsibly and professionally. Remember, your communications reflect on the entire organization.
- **Data Sensitivity:** Always encrypt emails containing confidential or sensitive information. This ensures that only intended recipients can access the contents.
- **Attachment Handling:** For large files or attachments, avoid sending them directly via email, which can strain the system. Instead, use approved cloud storage, intranet links, or other provided tools to share them.
- **Opinions:** Ensure personal opinions are not mistaken as official statements from the Group. If an email contains significant legal or confidential implications, mark it as "confidential" or "subject to contract."

9.2. Email Forwarding

- **Manual Forwarding:** Forwarding emails containing sensitive or confidential information is permissible only under the following conditions:
  1. There's a legitimate business need.
  2. Appropriate security precautions, like encryption or secured channels, are employed.
- **Prohibition on Auto-Forwarding:**
  1. Do not use automation tools, protocols, or rules (e.g., POP, IMAP) to auto-forward emails, especially outside of the organization.
  2. An explicit exception in writing from the IT Policy Committee is required to deviate from this rule.
- **Personal Email Accounts:** Using personal email accounts or individual servers for business-related communications is forbidden. Such practices can pose a security risk. Exceptions can only be made with written approval from the IT Policy Committee.

Any violations of the above guidelines can have severe consequences. If unsure about any procedure or facing challenges, always reach out to the IT Department or your supervisor for guidance.

9.3. Misuse

Examples of improper uses include:

- Concealment or misrepresentation of names or affiliations (e.g., misrepresenting oneself as another user).
- Use of email to send spam.
- Alteration of source or destination address of email.
- Use of email for partisan political or lobbying activities.
- Use of email for personal commercial activities or personal gain.
- Use of email to violate the Group policy on harassment and discrimination.
- Use of email to violate the law.

10. Backup and Disaster Recovery

10.1 Work-Related Data Storage

Only work-related data and electronic files may be stored on the Group's systems. Personal files, such as photos, videos, or non-work-related documents, should not be stored on the Group's devices. The Group reserves the right to monitor, assess, or delete any files stored on its systems.

10.2 Personal File Management

While the primary responsibility is to ensure work-related data storage, employees should also be cautious about their personal data. It's advisable to keep personal and work data separate, not just for professional reasons but also to ensure that personal data doesn't get mistakenly deleted during routine system maintenance or data purges.

10.3 Backup Procedures

The Group maintains a regular backup policy for data stored on its primary servers. However, employees are also responsible for ensuring that crucial data stored on individual laptops or workstations, especially those not frequently connected to the network, are periodically backed up. Employees can contact the Group IT Department for assistance or guidance on proper backup procedures.

10.4 Disaster Recovery Plan

The Group has a disaster recovery plan in place to ensure the continuity of its operations in the event of system failures, data loss, or other incidents affecting its IT infrastructure. Employees should familiarise themselves with the disaster recovery plan and their specific roles and responsibilities during recovery. The plan will be regularly tested and updated to ensure its effectiveness.

11. Training and Awareness

11.1 Employee Education

The Group is committed to ensuring all employees have the knowledge and skills to use IT systems and services securely and efficiently. As part of this commitment, employees may be required to participate in regular training sessions provided by the Group or other authorised sources. These sessions aim to keep employees updated on the latest IT procedures, technologies, and potential threats.

11.2 Security Awareness

Recognizing potential security risks associated with IT systems and services is paramount. This includes threats like phishing attacks, malware, and unauthorized access. The Group will provide ongoing security awareness training or updates to educate employees on current threats and best practices. This not only helps employees identify threats but also instructs them on the appropriate response in the case of a security incident.

11.3 Phishing Drills and Training

- **Objective:** To prepare and educate employees about the risks of phishing attacks, the Group will conduct periodic simulated phishing campaigns. These simulations are designed to gauge employee readiness against such threats and are not punitive in nature.
- **Procedure:** Employees who click on simulated phishing emails will be provided with additional training to help them identify real-world phishing attempts in the future. This iterative process ensures that the entire organization becomes more resilient against phishing threats over time.
- **Feedback Loop:** Post-drill analysis will be shared with the Group to highlight areas of improvement and further strengthen our defenses against such cyber threats.

11.4 Continuous Feedback and Improvement

The Group encourages a feedback loop, allowing employees to actively participate in continuously improving IT policies, training methodologies, and general practices. Feedback, questions, or suggestions for improvements can be directed to supervisors or the Group IT Department. Collaborative efforts ensure that our IT environment remains secure, efficient, and compliant.

12. Glossary of Terms

Keywords	Description
Policy Custodian	Refers to the role and responsibility of updating and maintaining the policy document accurate and aligned with the group's corporate governance strategy.
Cluster IT Manager	Position held by appropriate persons with responsibility of managing IT and security risks within each company or entities within the Group.
Users	Employees, trainees, permanent or temporary staff, business partners, subcontractors or any authorised person by the group to interact with the group's information processing facilities or process information for the group through its information systems.
Phishing	Refers to the fraudulent attempt of obtaining confidential information from users through tricks over phone calls, emails or even text messages.
Malware	Refers to any malicious software that is harmful to a computer systems and users. Example of malware are computer viruses, Trojan horses, spyware, ransomware, computer worms.
Advanced Threat Protection	Refers to state of the art capability of information systems to combat malware through advanced techniques.
Virus	A type of malware that spreads by inserting itself into other programs or files.
Spyware	Malware that covertly gathers information about a user's system without consent.
Ransomware	Malware that encrypts data on a device or system until a ransom is paid.
Security Incident	A violation or imminent threat to security policies, procedures or technology.
Data Breach	An incident where sensitive or confidential data is accessed without authorization.
Multi-Factor Authentication	Requiring two or more forms of identification to verify a user's identity.
Remote Wipe	Remotely deleting data from a device when it is lost or stolen.
Acceptable Use	Permitted uses for IT resources according to security and ethics policies.
Role-Based Access Control	Managing access to IT resources based on user roles and responsibilities.

(Version 2023 – V2.4)

Governing the use of computers, computer services, and communication devices, including email and Internet

I, ____, hereby acknowledge having read and understood the Information Technology Policy, governing the use of computers, computer services and communication devices, including e-mail and Internet, and that I agree to be bound by the terms outlined in it.

Date: _________________

Employee's signature: ____________________________