# TERRA MAURICIA LTD

## Information Technology Policy

For the future. From 1838

terra

# INFORMATION TECHNOLOGY POLICY

## (Version 2020 – V1.8)

## Governing the use of computers, computer services, communication devices, including e-mail & Internet

All hardware, software, applications, computing services, data, electronic files and communication devices, collectively referred to as "information systems", "systems" or "services", and which are provided to employees are considered to be the property of Terra Mauricia Ltd and its subsidiaries, referred to as the "Group".

As such, data and electronic files can be subject to review and/or monitoring, without permission of the employee. Data and electronic files include, but are not limited to, all files located on computers, servers, storage appliances, cloud services and communication devices, copied or created by applications and other mediums including e-mails sent and received through the Group's e-mailing systems.

All employees who use the Group's information systems must do so in a responsible and legal manner. Moreover, all employees are responsible for maintaining the Group's integrity and reputation when using these systems.

This policy is intended to help each employee fulfil these responsibilities and may be regarded as an 'ELECTRONIC CODE OF CONDUCT'. This document is not superseding any other code of conducts, procedures, manuals, ethical code of conduct already implemented within the Group.

The content of this 'ELECTRONIC CODE OF CONDUCT' is non-exhaustive and may be revised as often as the Group sees fit in regard to new technological advances or other reasons.

**The Group takes this matter seriously and failure to observe this policy may result in disciplinary actions.**

**Context**

The Group encourages you, within the guidelines set out below, to explore for work purposes the potential of the electronic tools which has been provided to you. The systems and services provided by the Group are for business purposes only. You may not use them for personal gain or to express personal opinions. You must remember that when using these systems, particularly e-mail and Internet, you are representing the Group to the outside world.

**Software**

Software includes and is not limited to licensed software, OEM licenses, freeware, apps and open source packages. The legal requirements governing software use and distribution are complex and various. Therefore, great care must be taken, particularly when copying and installing software. Illegal copying of software is considered theft. Copyright laws govern the ownership and use of software. Infringement can lead to criminal prosecution and liability for damages.

Be aware that it is not only common programs such as Microsoft products that are controlled by licensing agreements, but also items such as fonts, templates, drivers, sound files, graphics, logos and screen savers.

Please remember it is not what you consider reasonable use of the software, but what has been agreed to, however unreasonable this may seem, in the licensing agreement governing its use. Please seek advice from the Group IT Department if in doubt.

In addition to causing the Group to be in breach of copyright law, copying of unauthorised software can also affect the integrity of the Group computer systems by introducing software that is incompatible with those systems or which might carry computer viruses or other hazards.

To avoid these dangers:

- You are not allowed to install any software on the Group's systems. Only authorised IT personnel from the Group IT Department can do so.
- Do not attempt to download any software on any machine or device belonging to the Group without prior approval from the Group IT Department.
- Do not copy software from an office computer or systems to your personal home computer (or vice-versa) without the prior consent of the Group IT Department.

**E-mail & Internet**

The Internet is not a secure medium, and all messages created, sent, or received over e-mail and the Internet is, therefore, considered unsecured information.

If you need to send confidential information via email, we recommend using encryption. The facility to encrypt emails is provided and should be used. If you require assistance for sending confidential information over emails, you can seek advice from the Group IT Department.

The Group reserves the right to monitor or access any system and delete messages or files on any of these systems.

The Internet and other systems may not be used to access or create pornographic material. No abusive, profane, or offensive material in any form (pictures, sound, text, video, e-mail, etc.) may be stored in or transmitted through any part of the Group's systems and network.

Likewise, the Group through its Group IT Department reserves the right not to grant access to specific Internet resources, which are and are not limited to, non-work related, non-productive, offensive, abusive, profane and bandwidth intensive.

Never download software from Internet or e-mail without the permission of the Group IT Department, because you may unwittingly introduce a computer virus into the Group's systems or otherwise disrupt the stability of your computer or the entire system. Never provide access to third parties to the network, Internet connection or systems unless the Group IT Department has provided an official authorisation.

E-mails are not designed to transfer large files. It is your responsibility to ensure that the attachment file size is reasonable before sending an e-mail. If in doubt, please contact the Group IT Department for assistance. Do not send multiple e-mails with smaller attachments believing that it will be a workaround. Sending multiple e-mails with attachments to external recipients is often considered as mass-mailing and may result in the blacklisting of our domain names and public IP address. Remember that companies to which an e-mail is sent have filters/policies set. As such, these companies have the right to reject e-mails which are considered too large or which may contain specific keywords.

Do not present personal opinions as being representative of the Group. E-mails are permanent written records capable of widespread publication. They can be used as evidence in court (e.g., in a libel action). Under certain jurisdictions, e-mails can be used as evidence of a contract. If in doubt, mark communications "subject to contract". Mark e-mails containing sensitive information as "confidential". Where appropriate, consider using password protection for enclosed documents.

Do not read other people's e-mails without their express permission. Immediately delete e-mails which may have reached you in error. Do not use e-mail for unauthorised mass-mailing or joining subscriber lists indiscriminately as that can put a strain on the e-mailing systems and other computer resources.

Do not use e-mail or the Internet, or any other electronic means, to engage in harassment of any kind for any reason against any group or individual. Remember that what you consider to be banter, another may consider harassment.

**Copyright**

Unauthorised copying of a third party's property, including making a hard copy or electronic copy or simply storing the work without the permission of the owner, constitutes infringement of copyright.

You may not freely copy works available on the Internet, Intranet or other group systems. Copying third party property may expose the Group and yourself to action for infringement, including a claim for damages.

Do not use a third party's brand or business name without prior permission. Do not take unfair advantage or use them in a manner that is detrimental to the character or reputation of that brand or name.

Do not reproduce copyrighted material without authorisation from the copyright owner.

**Data Protection Act**

Terra is duly registered as a data controller/processor with the Data Protection Office of the Republic of Mauritius.

Consequently, Terra abides to the regulations set out in the Data Protection Act (2017) and General Data Protection Regulation (GDPR) of the European Union (2018) by ensuring that personal data pertaining to data subjects are lawfully obtained and processed for legitimate purposes.

Likewise, the Group through its Group IT Department reserves the right not to grant access to specific Internet resources, which are and are not limited to, non-work related, non-productive, offensive, abusive, profane and bandwidth intensive.

Never download software from Internet or e-mail without the permission of the Group IT Department, because you may unwittingly introduce a computer virus into the Group's systems or otherwise disrupt the stability of your computer or the entire system. Never provide access to third parties to the network, Internet connection or systems unless the Group IT Department has provided an official authorisation.

E-mails are not designed to transfer large files. It is your responsibility to ensure that the attachment file size is reasonable before sending an e-mail. If in doubt, please contact the Group IT Department for assistance. Do not send multiple e-mails with smaller attachments believing that it will be a workaround. Sending multiple e-mails with attachments to external recipients is often considered as mass-mailing and may result in the blacklisting of our domain names and public IP address. Remember that companies to which an e-mail is sent have filters/policies set. As such, these companies have the right to reject e-mails which are considered too large or which may contain specific keywords.

Do not present personal opinions as being representative of the Group. E-mails are permanent written records capable of widespread publication. They can be used as evidence in court (e.g., in a libel action). Under certain jurisdictions, e-mails can be used as evidence of a contract. If in doubt, mark communications "subject to contract". Mark e-mails containing sensitive information as "confidential". Where appropriate, consider using password protection for enclosed documents.

Do not read other people's e-mails without their express permission. Immediately delete e-mails which may have reached you in error. Do not use e-mail for unauthorised mass-mailing or joining subscriber lists indiscriminately as that can put a strain on the e-mailing systems and other computer resources.

Do not use e-mail or the Internet, or any other electronic means, to engage in harassment of any kind for any reason against any group or individual. Remember that what you consider to be banter, another may consider harassment.

**Copyright**

Unauthorised copying of a third party's property, including making a hard copy or electronic copy or simply storing the work without the permission of the owner, constitutes infringement of copyright.

You may not freely copy works available on the Internet, Intranet or other group systems. Copying third party property may expose the Group and yourself to action for infringement, including a claim for damages.

Do not use a third party's brand or business name without prior permission. Do not take unfair advantage or use them in a manner that is detrimental to the character or reputation of that brand or name.

Do not reproduce copyrighted material without authorisation from the copyright owner.

**Data Protection Act**

Terra is duly registered as a data controller/processor with the Data Protection Office of the Republic of Mauritius.

Consequently, Terra abides to the regulations set out in the Data Protection Act (2017) and General Data Protection Regulation (GDPR) of the European Union (2018) by ensuring that personal data pertaining to data subjects are lawfully obtained and processed for legitimate purposes.

Employees who manage and have access to personal data as part of their respective jobs are required to abide to the Data Protection Act (2017) principles.

From a broad perspective, this means that personal data related to data subjects should be obtained through written consent and clear explanations should be provided to data subjects about the purpose of collecting and processing such personal data.

Personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is collected and processed. Personal data for children under the age of 16 should not be collected nor processed unless the consent of a parent, guardian or next of kin is officially obtained. Employees and Business Units (BUs)/subsidiaries shall maintain a record of all processing operations under their responsibilities.

In exceptional cases, relevant personal data which is required for performing obligatory processing (e.g., payroll) can be collected without the explicit consent of the data subject. However, it is highly recommended to enquire with the designated Data Protection Officer (DPO) at Terra to ensure compliance with the law.

It is important that BUs/subsidiaries perform a Data Protection Impact Assessment (DPIA) for all projects in which the rights and freedoms of data subjects are at stake. The Data Protection Officer at Terra must be informed about these projects.

The Data Protection Officer at Terra should also be immediately informed, where applicable, of any personal data breach in a timely manner.

**Data storage**

Only work-related data and electronic files may be stored on the Group's systems. You may not use the Group's systems for storing personal photos, games, videos, downloaded software, pornography, joke material, or items of a distasteful or offensive nature. The Group reserves the right to monitor, assess or delete any files, whether maintained on the network, server or on the workstation you use.

The Group maintains a policy for backing-up data and information stored on servers; however, if data is stored on your laptop or workstation, it is your responsibility to ensure that is backed-up. Please contact the Group IT Department if in doubt.

**Laptops & mobile devices**

You may use the Group's IT assets (workstations, laptops and mobile devices) outside the premises only with permission from your immediate supervisor and/or head of department. If in doubt, please contact the Group IT Department for advice.

Laptops and mobile devices must be used responsibly and always kept secure, particularly when left unattended. Do not forget to remove disks, flash drives and other peripherals from the laptop when not in use and store them securely. Always carry the laptop in its case to protect it from damage.

**Usernames & passwords**

You are responsible for your usernames and passwords. Do not share your username and password and never let anyone use yours. It is your responsibility to memorise your username and passwords and do not write them down. If temporary passwords are required, make sure they are held safely until changed or cancelled. Change your password immediately if you suspect that it has been compromised. Do not use passwords that can be easily guessed (e.g. "password", date of birth, other personal data, etc.).

Your password should meet a certain complexity level i.e., it must include a minimum of 8 alphanumeric characters comprising lower, upper case and at least one special character.

You will be requested to change your password every 60 days, but you may also do it before the reminder. The Group reserves the right to alter and enforce password policies for different applications and systems. It is recommended not to use the same passwords (or variation of the same passwords) repeatedly. Do not store your password in programs or on unprotected electronic files. Remember, you are the only employee that can gain access to your computer using your own password.

A member of the Group IT Department may request your password to intervene on your workstation/laptop. Please change the password immediately when the intervention is completed.

**Viruses and other threats**

A computer virus is a program designed to corrupt or destroy other programs, software, systems or files. A virus is transmitted via electronic means which include the internet local corporate network, flash drives, optical medias, external hard drives and e-mails.

The Group IT Department has installed a next generation endpoint protection software to protect your computer. . Although this software operates in a non-intrusive way, it will inform whenever a suspicious activity is encountered. You do not have to take any actions, but it is safe to inform the Group IT Department whenever this is the case for further investigation. Moreover, you must not attempt to tamper, disable or remove this software from your computer. If you believe your next-generation endpoint protection is not operating, you should inform the Group IT Department immediately.

You are reminded that you need to seek advice and authorisation from the Group IT Department before attempting to install/try any demonstration/free software, applications or programs on your computer.

**Personal use of computers**

Incidental and occasional personal use of company computers is allowed for reasonable activities that do not require substantial hard disk space, network bandwidth or other computer equipment and is not harmful to the Group's activities or belongings. In any other case, the use of company computers on a personal basis shall be subject to an authorisation from the Group IT department.

The above policy is intended to help you make the best use of the system and services at your disposal while allowing the Group to conduct itself in a legal, secure, and reputable manner. If you have any questions on interpreting this policy, or can point to improvements or omissions, please contact your immediate supervisor or the Group IT Department.

**INFORMATION TECHNOLOGY POLICY**

**(Version 2020 – V1.8)**

**Governing the use of computers, computer services, communication devices, including e-mail & 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 & Internet, also referred to as 'electronic code of conduct', and that I agree to be bound by the terms set forth in it.

I further understand that this document cannot and shall not constitute a contract of employment.

Date: _____

Employee's signature: _____