VUNANI

LIMITED

INFORMATION TECHNOLOGY (IT)

POLICY

GLOSSARY

Anti-virus	-	Computer software used to prevent, detect and remove malicious software.
Auto signature	-	Employee and company contact information that is appended automatically to the end of an e-mail message.
Corporate network	-	Physical (Ethernet cable), remote and wireless access to Vunani JHB and CT systems and resources.
Desktop items	-	Items on the main screen area that you see after you turn your computer on and log onto Microsoft Windows.
Documents folder	-	Microsoft Windows folder allocated to help employees store data files. Does not include Music, Pictures, Videos and Desktop items.
Encrypt	-	Convert data into another form which cannot be easily understood\accessed by anyone except authorized parties.
FTP Site	-	A File Transfer Protocol Site is used to transfer files from one host to another host (normally via the internet)
IT department	-	Internal IT Team - ITHelpdesk@vunanigroup.co.za or 011 263 9555
IT equipment	-	Electronic devices that are used in the operations of business and connected to the Vunani Corporate Network i.e. computers, laptops, tablets, smartphones, printers, fax machines, routers, switches, wireless access points, hubs, servers, firewalls etc.
Operating system	-	Software that manages all other programs on a device e.g. Windows,OS Android, IOS etc.
Out of office	-	Microsoft Outlook feature also known as Automatic Replies which enables an employee to have e-mail automatically responded to when out of the office regardless if the computer is on or off.
Passwords	-	A secret word or string of characters used for user authentication to prove identity or gain access to a resource.

Patches	-	Piece of software designed to update a computer program to fix security vulnerability and improve usability.
Pirated software	-	Software that is obtained illegally or not properly licensed.
Portable equipment	-	Laptops, smartphones and projectors.
Private keys	-	Special code used to encrypt\decrypt data
Remote wipe	-	Security feature that allows the IT department or the device owner to send a command to a device remotely to delete data.
Save	-	Intentionally storing unencrypted passwords on your computer and selecting “Save Password” when prompted to do so.
Special characters	-	A character that is not a letter or number e.g. *&^%$!.
USB drives	-	Portable data storage device.
User accounts	-	An account used by an employee to gain access to a system or resource.
Virus definition file	-	Updated anti-virus file used to detect and disinfect the latest viruses and other malicious software.
Virus, worm, trojan horse	-	Software programs that are designed to interfere with computer operations and cause damage to data and systems.

INTRODUCTION

This document serves to outline the company's policy on the acceptable use of IT equipment and IT Systems. The IT equipment and systems are to be used for business purposes in serving the interests of the company, and of our clients in the course of normal operations. The purpose of the policy is to protect Vunani and its employees. Inappropriate use exposes Vunani to risks including but not limited to, virus attacks, compromise of network systems and services, reputational damage and legal issues.

RESPONSIBILITY

This policy applies to all Vunani employees, contractors, business partners or anyone accessing the Vunani corporate network and third-party systems.

ACCEPTABLE USE POLICY

1. **General Use and Ownership**

1.1. IT Equipment

Whilst the IT department desires to provide a reasonable level of privacy, employees should be aware that the data they create on the company systems, remains the property of Vunani.

Employees are responsible for exercising good judgement regarding the reasonableness of personal use.

For security and network maintenance purposes, the IT department may monitor equipment, systems and network traffic at any time.

Vunani reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Use of Vunani equipment is strictly applicable to the company employee and any use by third parties is prohibited. All authorised employees must ensure that equipment is only used by themselves and for the purpose for which it is intended.

Employees are expected to take all appropriate measures and precautions to prevent the loss, theft and/or unauthorised use of portable equipment.

1.2. E-mail

E-mail and instant messaging tools provided to employees must not be considered as a means of exercising the right of free speech. It is prohibited to display or transmit the following:

i. Offensive, defamatory, discriminatory or harassing material.
ii. Sexually explicit or other offensive images or jokes.
iii. Unlicensed copyright material.
iv. Non-business related video and image files.
v. Private and personal advertisements.
vi. Chain letters.
vii. Do not send or forward e-mail notices concerning virus or harmful code warnings to other Vunani employees. This type of communication will be distributed via the IT department.
viii. Vunani messaging infrastructure will not be used for politically motivated e-mail.
ix. Employees must not send or forward E-mails or postings that threaten, in any way annoy or abuse persons, legal entities, countries, nations, ethnicities, sexual orientations, religions, political beliefs, as well as mental and physical disabilities and in general messages that might have legal or other consequences for the company's public image.
x. Employees must not use vulgar, coarse, and abusive or any other inappropriate language towards colleagues, clients, competitors or others in their messages
xi. No deviation from the company standard auto signature is allowed. Refer to company brand guidelines.

Practice the following E-mail Etiquette:

i. Employees must enable their e-mail Out of Office if they are on leave, or away from their desks for an extended period of time.

ii. Unless absolutely necessary, refrain from Replying to all when responding to e-mail messages.
iii. When sending e-mails to multiple clients, use the BCC Field.

1.3. Internet

The use of internet services must reflect the mission of the company and support the company's goals and objectives. Employees are required to use their common sense and exercise their good judgement while using Internet services. Bandwidth both within the company and in connecting to the Internet is a shared, finite resource. Employees must make reasonable efforts to use this resource in ways that do not negatively affect other employees.

The following uses of company provided Internet access are **not** permitted:

i. Use the internet for private financial gain.

ii. Use of the internet leads to degradation or disruption of network performance.
iii. Use the internet to download or distribute pirated software or data.
iv. To deliberately propagate any virus, worm, Trojan horse or trap door program.
v. Download entertainment software or games, or play games against opponents over the Internet or network.
vi. Audio and video streaming are not permissible unless it is explicitly business related, however the use should be kept as a minimum because of the high bandwidth utilisation.
vii. Peer to peer connections and proxy avoidance sites are strongly prohibited.
viii. Access FTP sites for personal use.
ix. Do not save company private keys, passwords, credit card details etc.
x. Posting information on websites that is defamatory to the company, its products\services, colleagues and\or customers.

Any software or files downloaded via the Internet onto the company network, becomes the property of the company if bought by Vunani. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

Employees may not download software or data larger than **20MB**. Employees must arrange with the IT department if they wish to download files larger than 20MB.

2. **Information Security**

Passwords must be kept secure and user accounts should not be shared with anyone else. The minimum password length is **8** characters and must contain both upper and lower case letters and special characters. Passwords must be changed every **30** days. User accounts will be locked out after **3** invalid attempts. Employees are responsible for the security of their passwords and user accounts. Do not reveal your password to anyone (including the IT Department) Any employee suspecting that his/her password may have been compromised must report the incident to the IT department and change all passwords.

All desktops and laptops with the exception of Bloomberg and Reuters computers, should be locked by pressing **ctrl-alt-del** on the keyboard when left unattended. After **10** minutes of inactivity, the computer will lock automatically. Information contained on portable computers is especially vulnerable, special care should be exercised.

All equipment that connects to the Vunani network shall have anti-virus installed and is up to date with the latest virus definition file as well as security patches for the

operating system and applications. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses.

In the event of lost\stolen equipment, the incident must be reported to the police and the IT department must be informed accordingly. It is the manager's discretion with regards to the appropriate steps that will be taken against the employee.

3. **Backups**

Computers and laptops are not automatically backed up by the IT department. All business related documents must be saved in the **Documents** folder on your computer.

This folder synchronises with the server and the servers are backed up daily. No personal data such as movies, videos, pictures etc. may be saved in this folder.

Employees should backup at least daily when working away from the company network. Use USB drives as necessary to back up data but always encrypt and store the data securely. Store the backup separately to your laptop and carry out frequent test restores.

4. **Personal Equipment**

Employees may use their personal devices to access the following company resources:

i. E-mail
ii. Calendars
iii. Contacts
iv. Documents
v. Applications

The IT department do not have the resources or expertise to support all possible devices and software. Employees will receive limited support on "best endeavor" basis for business purposes only.

The company will not be responsible for the running costs of the equipment including but not limited to hardware repairs, licensing of software, connectivity etc.

Equipment must be kept up to date with manufacturer or network provided patches and anti-virus, antispyware software. The device must be given an appropriate name e.g. Joe's phone or Sally's Tablet so that it can be identified and tracked on the network.

Remote wipe utility must be installed on the device and activated when the equipment is lost or stolen, when the employee terminates his/her employment or when the IT department detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

POLICY REVIEW

This policy will undergo a planned review at least annually or whenever the process has changed to ensure it is current and effective.