PROCEDURE AND POLICY MANUAL
INFORMATION TECHNOLOGY (IT) END USER POLICY

PURPOSE:
To effectively manage the use of IT equipment, Network and facilities within the Company.

RESPONSIBILITY:

- Managing Director
- Financial Manager
- IT Manager

1. INTRODUCTION

Computer information systems and networks are an integral part of business with Sandton Plant Hire (Pty) Limited ("the Company"). The Company made a substantial investment and financial resources to create and maintain these systems and networks and the integrity and operation thereof should be protected at all times.

The enclosed policy has been established in order to:

- Protect this investment
- Safeguard the information contained within these systems
- Reduce business and legal risk
- Protect the reputation of the Company and its clients
- Act as a guideline for our users

2. CONDITION OF EMPLOYMENT

Adherence to this Information Technology, Internet and Security End-user policy is a condition of employment. Contravention of this policy may result in disciplinary action in accordance with Company policy and the Company's disciplinary code and procedures.

3. ADMINISTRATION

The Information Technology Manager (IT Manager), Managing Director and Financial Manager responsible for IT, are responsible for the administration of this policy.

4. CONTENTS

The topics covered in this document include:

- Statement of responsibility
- The Internet and e-mail
- Computer viruses
- User accounts and passwords
- Physical security
- Software copyright and license agreements
- Home and mobile use

5. STATEMENT OF RESPONSIBILITY

General responsibilities pertaining to this policy is set forth in this section. The following sections list additional specific responsibilities.

5.1 Manager responsibilities

IT Manager and Director/Financial Manager must:

- Ensure that all appropriate employees are aware of and comply with this policy.
- Create appropriate performance standards, control practices and procedures designed to provide reasonable assurance that all employees observe this policy.

5.2 IT Manager Responsibilities

The IT Manager must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

6 THE INTERNET AND E-MAIL USAGE POLICY

The Internet is a very large, publicly accessible network that has millions of connected users and organizations world-wide. The World Wide Web (WWW) is a subset of the Internet and is a collection of interlinked documents and multi-media files.

6.1 Policy

Access to the internet is provided to employees for the benefit of the Company and its business. Employees are able to connect to a variety of business information resources around the world, through the WWW. Internet access through the Company's network is limited to the Company's employees and other that the Company may authorize.

Conversely, the Internet and WWW is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the Company's interest the following policy has been established for using the Internet and e-mail.

6.2 Acceptable use

Employees using the Internet including e-mail are representing the Company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using web browsers to obtain business information for Company use from commercial or academic web sites.
- Accessing databases for information as needed for the Company's business.
- Using e-mail for business contacts.
- Utilizing the Internet, including e-mail, as a tool to advance the business objectives of the Company.

6.3 Unacceptable use

Employees must not use the Internet or e-mail for purposes that are illegal, unethical, harmful to the Company (including statements, actions or omissions that do, or could, lead to civil and/or criminal liability to the Company or damage or loss to the Company or its reputation or fellow employees). Examples of unacceptable use are:

- Viewing, accessing, copying, processing or transmitting any content or material that is offensive, harassing, fraudulent, illegal or obscene including any pornography, hate mail, racist remarks or hoaxes to any Company employee, trading partner, clients or anybody else.
- Accessing any Social Networking site, such as Facebook, Twitter, WhatsApp, Tweet Deck, Digg, Bebo, Ning, HI5, myspace, orkut, LinkedIn etc. on the Company network is strictly prohibited.
- Sending or forwarding chain e-mail, for example, e-mail messages containing instructions to forward the message to others when not for official or Company business purpose (chain letters). This includes the broadcasting of e-mail, i.e., sending the same message to more than 5 recipients or more than one distribution list if not specifically work related.
- Sending forwarding joke e-mails, electronic greeting cards, Christmas Cards, music files (e.g. MP3), video clips (not related to official business) and games.
- Sending or receiving unusually large e-mails – acceptable size is 5 MB or less.
- Representing personal opinions as that of the Company via e-mail or publication of unauthorized statements onto web sites, bulletin boards, discussions areas or newsgroups.
- Conducting a personal business using Company resources.
- Conducting any form of campaign against fellow employees or any third party by e-mail.
- Using a third-party e-mail provides, i.e. “Hotmail”, “Yahoo mail”, “Gmail” or any other e-mail service provided by any outside Internet Service Provider or party, to send Company information or any files emanating from within the Company to external parties.
- Using an Internet file storage facility such as “Dropbox”, “Google Drive”, “DiskOnNet”, etc., to make backups or copies of files from the Company onto the Internet. The IT Manager will provide adequate facilities for the employee to store and make backups of crucial working files. Approval for using these facilities can be obtained from the Financial Director.
- Providing computing or storage resources, including file sharing or swapping, to external parties through parties such as “Napster” and “Gnutella”.
- Using a modem whilst connected to the Company’s internal network – under no circumstances is any modem (3G or Mobile Phone) allowed to be used when a workstation or laptop is connected directly to the Company’s network.
- Breaking through security controls, whether on Company official equipment, personal Laptop or on any other computer system connected to the network;
- Accessing Internet traffic (such as e-mail) not intended for him/her, even if not protected by security controls, or doing anything which would adversely affect the ability of others to access the Internet/Intranet resource they are entitled to access;
- Intentionally or recklessly accessing or transmitting computer viruses and similar software;
- Intentionally or recklessly accessing or transmitting information about, or software designed for, breaching security controls or creating computer viruses;
- Passing of internal e-mail distribution lists to outside agencies and organizations;

Intentionally or recklessly accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to the Company's policy (except where this is strictly and necessarily required by the job, for example within the social services or consumer protection areas, where

- sometimes specifically authorized and required to research into illegal activities. The excuse of personal or private research would not be acceptable);
- Knowingly doing anything which is illegal under South African law or the law of any other relevant country (including, for example, downloading pirated music or videos);
- Political lobbying of any kind;
- Personal business for financial/commercial gain;
- Betting, wagering or gaming
- Downloading games
- Hacking or accessing private external networks from within the Company network.
- Any activities which could cause congestion and disruption of networks and systems, e.g. Accessing YouTube;
- The use of aliases is not permitted in official activities.

6.4 Employee responsibilities

The Company employees may access the Internet through the Company's network for the purpose of conducting Company business. Viewing, copying, storing or sending content outside of the scope of the Company employment is prohibited. The Company provides Internet access through the Company's network to Company employees as a privilege that is based on adherence to the Company's policies and rules regarding Internet access. In addition to being responsible to abide by the conditions as set out in the end-user policy, including but not limited this paragraph an employee who uses the Internet or Internet e-mail shall:

- Ensure that all communications do not interfere with his/her or any other employee's productivity.
- Be responsible for the content of all text, audio, images or videos that he/she places on or sends over the Internet.
- Not transmit copyrighted materials without permission of the author thereof or without defining and acknowledging the owner thereof.
- Know and abide by all applicable policies dealing with security and confidentiality of Company and client records.
- Avoid, where possible, transmission of information confidential to the Company or its clients. It is necessary to transmit confidential information; employees are required to take steps to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate purpose.
- Report any form of irregularity or transgression of this end-user policy (e.g. receipt of objectionable e-mail) to the Company IT Manager, Financial Director or alternatively the Managing Director.

Email Usage Policy

The Company has introduced the Microsoft Exchange Email Server facility to provide its employees with an e-mail facility. But this facility also provides an extremely flexible set of office tools such as diary, meeting scheduler, and task management. These tools provide a wealth of opportunities to streamline many administrative tasks.
This coupled with the implementation of electronic service delivery will mean that much less reliance will be placed on *"paper-based"* systems, especially as electronic signatures become legally binding.
The following guidelines are aimed to ensure that staff applies a more uniform management practice to their e-mail usage:

- All e-mail users have the facility to print hard copies of their e-mails they have sent or received. For that reason, it is unnecessary to send hard copy *follow-up's* in most cases.

  However, in certain circumstances, such as contract or other legal documents, this may be insisted upon.

- The Company has a corporate standard for replies to all letters, faxes and e-mails of 5 working days.

- E-mails should be read regularly. When it is known that this will not be possible for an extended period (e.g. leave), the re-direction or 'out of office' facilities available should be used. The IT Manager / 3rd Party IT Company can advise you further on using these tools.

- As specified under "e-mail disclaimer" employees must be careful to avoid sending or forwarding sensitive or confidential information via e-mail and is advised not to do so unless confidentiality can be guaranteed.

- All e-mails are held on a central server and will be backed up automatically each night.

- Regularly delete old or unwanted e-mails, messages and documents. This will help ensure that the performance of the network is maintained at a satisfactory level. The IT Manager / 3rd Party IT Company can advise you on such matters.

- Reasonable personal use of e-mail is permissible. However, the considerations/restrictions as set out within this policy still apply and this usage will be monitored by the IT Manager and reported to management accordingly.

- Private email addresses must be used to register with online social networking services such as Facebook, Myspace, Twitter or Instagram rather than your Company e-mail address.

The golden rule is that if you are unsure as to whether or not any particular usage is permitted you should always seek prior approval from IT Manager / 3rd Party IT Company.

The highest risk of exposure to an allegation of misuse will usually arise from lone or secretive use without your colleagues knowing what you are doing. E-mail must not be used for any of the following purposes:

- Accessing e-mail not intended for him/her, even if not protected by security controls, or doing anything which would adversely affect the ability of others to access e-mail resources to which they are entitled;
- Accessing of private mail or mailboxes on the Company network is strictly prohibited.
- Intentionally or recklessly accessing or transmitting computer viruses and similar software;

- Intentionally or recklessly accessing or transmitting information about, or software designed for, breaching security controls or creating computer viruses;
- Intentionally or recklessly accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence, or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to the Company's IT Security Policy (except where this is strictly and necessarily required by the job, for example within the social services or consumer protection areas, where employees are sometimes required to research into illegal activities. An excuse of personal or private research would not be acceptable);
- Knowingly doing anything which is illegal under South African law or the law of any other relevant country;
- Automatic re-direction of e-mails to service providers outside the Company's control/policy and legislative jurisdiction;
- Political lobbying of any kind;
- Personal business for financial/commercial gain;
- Any activities which could cause congestion and disruption of networks and systems;
- The use of aliases is not permitted in any official activity.

The IT Manager, after due consultation with the 3rd Party IT Company, reserves the right to recommend the following:

- Withdraw the employee's access to any computer systems and communication services, including e-mail services, if it is found that an employee is using e-mail for any of the above purposes. He/she may be subject to disciplinary action, in line with the Company's disciplinary procedures as governed by Personnel, in addition to being required to pay any appropriate part of costs incurred.

The IT Manager, after due consultation with 3rd Party IT Company, may recommend the following response to violations of the above policies by any combination of:

- Informal warning;
- Disciplinary action, potentially for gross misconduct, through the normal disciplinary process;
- Provision of information to the police for possible criminal proceedings.

The distribution of any information through the e-mail and messaging systems is subject to the scrutiny and monitoring of the IT Manager. The IT Manager and/or the 3rd Party IT Company, in-conjunction with the HR Department reserve the right to determine the suitability of this information.

The Company reserves the right to monitor and examine the contents of any part of its systems (including computer files, voicemail messages, email messages, Internet logs and the like) and to monitor usage of the email system. Surveillance and inspections can be conducted by management with the assistance of the 3rd Party IT Company and/or any person designated by the Chief Executive. The content of any email messages sent or received through the System is logged and may be monitored by the Company.

Any records created as a result of this surveillance will only be:

- used or disclosed for a legitimate purpose relating to the employment of employees or the legitimate business activities or functions of the Company.
- disclosed to law enforcement officials in connection with the detection, investigation or prosecution of an offence;
- used or disclosed for purposes directly or indirectly related to the taking of civil or criminal proceedings; or
- used or disclosed where the Company reasonably believes it to be necessary to avert imminent threats of serious violence or substantial damage to property.

6.5 E-mail signature & disclaimer

To ensure that an e-mail message is properly identified apart from the sender's e-mail address it is compulsory that the sender place the following e-mail signature and disclaimer at the foot of each individual e-mail message.

- No color backgrounds or picture are permitted when sending e-mails

Name Surname
employee@sandtonplant.co.za

Job Title

Tel: 011-805-3084/5 (Ext)

SANDTON PLANT HIRE

Company Registration No: 1982/005699/07 P.O. Box 391574, Bramley, 2018

Please consider the environment before printing this email

www.sandtonplant.co.za Disclaimer

6.6 Copyrights & Downloads

Employees using the Internet are not permitted to illegally and/or wrongfully copy, transfer, rename, add, modify or delete protected works, information or programs. Employees are responsible for observing copyright and licensing agreements that may apply when downloading or distributing files, documents and software. Any copyrighted material attached to a message should identify the author and acknowledge his/her copyright.

Employees must obtain approval from the IT Manager and if necessary the Company's authorized personnel before downloading material for which a fee is requested. Failure to observe copyright or license agreements may result in disciplinary actions by the Company and/or legal action by the copyright owner.

6.7 Monitoring & Privacy

All messages created, send or retrieved over the Internet are the property of the Company and may be regarded as public information and the Company reserves the right to intercept, read and inspect the same if the Company believes, in its sole judgment, that it is justified to so in order to protect its business. Should any private information of the employee be contained in such message the Company agrees to honor such privacy, it being recorded that any messages which may be personal by nature may be accessed and used by the Company where such message cause harm to the Company and has the potential of causing harm and where the nature or content of the message is or is suspect to be contrary to this policy or is otherwise unlawful.

All communications, including text, video or audio clips and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. This means that you should not put anything into your e-mail message that you do not want on the front page of a newspaper or be required to explain in a court of law.

7 COMPUTER VIRUSES

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources. It is important to know that computer viruses are much easier to prevent than to cure. Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

7.1 IT Manager responsibilities

The IT Manager shall:

- Install and maintain appropriate anti-virus software on all computers. Virus updates are sent to employees by the IT Manager.
- Respond to all virus attacks, destroy any virus detected, and document each incident

7.2 Employee responsibilities

- Employees shall not knowingly introduce a computer virus into Company computers.
- Employees should be responsible for running the update as soon as possible after receiving the update if this does not happen automatically.
- Run a virus scan on any executable file(s) received through e-mail.
- Employees shall not load diskettes, CD-ROMS, DVD's, USB Storage Device or any other media type of unknown origin. All incoming media shall be scanned for viruses before they are read or executed.
- Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and notify the IT Manager to take corrective action.

8 USER ACCOUNTS AND PASSWORDS

The confidentiality and integrity of data stored on Company computers systems must be protected by access controls to ensure that only authorized employees have access. The access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

In addition, employees shall access the Internet in a manner that does not compromise the Company's network security. This includes the employees keeping his/her username and password secure, prohibiting access to intruders or viruses, and reporting any suspicious activity to the Company's IT Manager. Employees that want to download Internet content from a non-Company source must observe Company security procedures.

Password Policy

- All passwords, including initial passwords, must be constructed and implemented according to the following rules:
- it must be routinely changed
- it must adhere to a minimum length as established by the Company IT support Company
- it must be a combination of alpha and numeric characters

- it must not be anything that can easily tied back to the account owner such as: user name, identification number, nickname, relative's names, birth date, etc.
- it must not be dictionary words or acronyms
- password history must be kept to prevent the reuse of a password
- If the security of a password is in doubt, the password must be changed immediately.
- Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- Password change procedures must include the following:
- authenticate the user to the helpdesk before changing password
- change to a strong password
- the user must change password at first login
- In the event passwords are found or discovered, the following steps must be taken:
- Take control of the passwords and protect them
- Report the discovery to the network administrator

Password Guidelines

- Passwords must be changed at least every 42 days.
- Passwords must have a minimum length of 8 alphanumeric characters
- Passwords must contain a mix of upper and lower-case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#$%^&*_+=?/~`;:,<>|\).
- Passwords must not be easy to guess and they:
- must not be your Username
- must not be your employee number
- must not be your name
- must not be family member names
- must not be your nickname
- must not be your identification number
- must not be your birthday
- must not be your license plate number
- must not be your pet's name
- must not be your address
- must not be your phone number
- must not be the name of your town or city
- must not be the name of your department
- must not be street names
- must not be makes or models of vehicles
- must not be slang words
- must not be obscenities
- must not be technical terms
- must not be school names, school mascot, or school slogans
- must not be any information about you that is known or is easy to learn (favorite - food, colour, sport, etc.)
- must not be any popular acronyms
- must not be words that appear in a dictionary

- must not be the reverse of any of the above
- Passwords must not be reused within 12 password periods
- Account lockout threshold of 3 minutes will apply
- Passwords must not be shared with anyone
- Passwords must be treated as confidential information

Creating a Strong Password

- Combine short, unrelated words with numbers or special characters. For example: eAt42peN
- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute) For example:
- livefish - is a bad password
- L1veF1sh - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and i's substituted by 1's can be guessed
- l!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable

Disciplinary Action

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries and/or lead to the termination of employment relations in the case of contractors or consultants; dismissal for interns. Additionally, individuals are subject to loss of the Company Information Resources access privileges, civil, and criminal prosecution.

8.1 IT Manager responsibilities

The IT Manager shall be responsible for the administration of access controls to all Company computer systems. The IT Manager will process additions, and changes upon receipt of a written request from the employee's Director.

Deletions may be processed via a written request sent to the online help desk. The IT Manager will maintain a list of administrative access codes and passwords and keep this list in the Company safe. The IT Manager will maintain a copy of the backup offsite.

8.2 Employees responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID (username) and password.
- Shall not disclose password to others. Passwords must be changed immediately if it is suspected that it may have become known to others. Passwords should not be recorded or kept where they might be easily obtained.
- Should use passwords that will not be easily guessed by others.
- Should log out when leaving a workstation for an extended period and ensure that when a screensaver is used that is protected by a password that automatically activates after 5 minutes of inactivity on the computer screen.

8.3 Human resources / Payroll Administrator's responsibility

Human resources and Payroll Administrator should notify the IT Manager promptly whenever an employee leaves the Company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

9 PHYSICAL SECURITY

It is Company policy to protect computer hardware, software, data and documentation from misuse, theft, fraud, unauthorized access and environmental hazards.

9.1 Human resources responsibility

The policy below applies to all employees:

- Diskettes/media should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
- Diskettes/media should be kept away from environmental hazards such as heat, direct sunlight and magnetic fields.
- Environmental hazards to hardware such as food, smoke, liquids, high or low humidity and extreme heat or cold should be avoided.
- Since the IT Manager is responsible for all equipment installations, disconnections and modifications, employees are not to perform these activities.
- Employees shall not take shared portable equipment such as laptop computer out of the office without the informed consent of the Managing Director and IT Manager. Informed consent means that the Director knows what equipment is leaving, what data is on it, and for what purpose it will be used.
- Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty will be accountable for any loss or damage that may result.
- Under no circumstance may any other equipment be connected to the Company's network without prior, written approval by the Director.

10 SOFTWARE COPYRIGHT AND LICENSE AGREEMENTS

All software acquired for or on behalf of the Company or developed by Company employees or contract personnel on behalf of the Company is and shall be deemed Company property. All such software must be used in compliance with applicable licenses, notices, contracts and agreements.

Non-compliance with legislation dealing with intellectual property, including copyrights, such as the Copyright Act and with license agreements can expose the Company and the responsible employee(s) to civil and/or criminal liability. Unless otherwise provided in the applicable license, notice, contract or agreement any duplication of copyrighted software, except for backup and archival purposes, may be violation of law.

This policy applies to all software that is owned by the Company, licensed to the Company, or developed using the Company's resources by employees.

10.1IT Manager responsibilities

The IT Manager shall:

- Maintain records of software licenses owned by the Company
- Periodically (at least annually) scan Company computers to verify that only authorized software is installed.

10.2 Human resources responsibility

Employees shall not:

- Install software unless authorized by the IT Manager. Only software that is licensed to or owned by the Company is to be installed on Company computers. Under no circumstances will any assistance/support be given on unauthorized or illegal products.
- Copy software unless authorized and recorded by the IT Manager.
- Download and install software unless authorized by the IT Manager.

11 HOME AND MOBILE USE

Employees accessing the Company's network from home or during a business trip must ensure that he/she uses the necessary security software that will establish a secure communication to the Company's security system when retrieving e-mail or accessing the Company's systems. Under no circumstances is any other unauthorized user allowed to use this facility. Time spent online interacting with Company systems should be limited to the minimum.

Employees should take care when traveling, especially in aircraft, buses and any other mass transport, that external parties cannot read information off computer screens or personal digital assistants (PDA). Employees should therefore exercise the necessary care when working on Company related information in public or non-Company areas.

In the event of a PDA, workstation or laptop being stolen, this should be reported immediately to the Company IT Manager, to arrange for all security access to be suspended.

12 Company Wireless Access

Connecting to the Company's wireless network, with your cell phone or tablet, is not allowed, as this has a huge impact on the performance of the Company's network and poses a security risk to the Company's IT Systems. Employees can request access to the Company's wireless network, by sending an email to:

taryn@sandtonplant.co.za
petrus.roets@sandtonplant.co.za
it@sandtonplant.co.za

With a reason, why access is required.

If there are any aspects regarding this policy that are unclear please consult with the IT Manager

Employee / Contractor Agreement

I have received a copy of Sandton Plant Hire (Pty) Ltd Corporate Policy Guideline on e-mail/Internet acceptable use, policy SPHITPOL01. I recognize and understand that the Company's e-mail, Internet and/or intranet systems are to be used for conducting the Company's business only. I understand that use of this equipment for private purposes is strictly prohibited.

As part of the Sandton Plant Hire (Pty) Ltd organization and use of Sandton Plant Hire (Pty) Ltd gateway to the Internet and e-mail system, I understand that this e-mail/Internet corporate guideline applies to me.

I have read the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment / contract with the Company.

I am aware that violations of this corporate guideline on e-mail/Internet acceptable use may subject me to disciplinary action, up to and including discharge from employment.

I further understand that my communications on the Internet and e-mail reflect the Company, world-wide to our competitors, consumers, customers and suppliers. Furthermore, I understand that this document can be amended at any time.

_____
Signed

_____
Date

Tel +27 (0)11 805 3084 Fax +27 (0)86 508 0378 Email reception@sandtonplant.co.za
Physical Address 768 Pretoria Main Road, Midrand GPS Coordinates S 26 02.014 E 28 06.693
Postal Address P.O. Box 391574, Bramley, 2018 COMPANY REG # 1982/005699/07