SUBJECT: **INFORMATION SYSTEMS**

EFFECTIVE DATE: 16 AUGUST 2007 (Updated July 2023)

PURPOSE: The purpose of this policy is to manage the use of the Information Technology (IT) facilities provided by the company, and to prevent abuse.

1. INTRODUCTION

Computer information systems and networks are an integral part of business within the Astral Group. Substantial investment in human capital and financial resources had been made to create and maintain these systems and networks. The integrity and operation thereof should be protected at all times.

2.1 PURPOSE

The purpose of this policy is to manage the use of the Information Technology (IT) facilities provided by the company, and to prevent abuse. This policy specifically addresses the IT facilities and thus has to be read in conjunction with all other Astral; policies which govern the conduct of all staff in the employ of the company

This policy has been established in order to:

- Protect the company's IT investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the reputation of the group and its companies.
- Limit and manage the legal risks to which the group is exposed to.

2.2. INTENDED AUDIENCE

The intended audience for this policy includes:

- All employees of the Astral Group.
- All subcontractors that make use of Astral IT facilities.
- MIS Manager, IT Manager or Manager responsible for IT.
- All Managers and Supervisors.

2.3. CONDITION OF EMPLOYMENT

Adherence to this IT Policy is a condition of employment. Any Employee found to have violated these policies could be subject to disciplinary action as set out elsewhere in the Astral Policy Manual.

2.4. CONDITION OF CONTRACT

Adherence to the IT Systems End User Policy is a condition of any contract with any sub-contractors making use of the Astral IT facilities. Where appropriate such sub-contractors should be made aware of this policy whenever they are appointed. A failure by any of them to comply herewith shall constitute a breach of contract with resultant potential legal liability as recognised by law.

2.5 STATEMENT OF RESPONSIBILITY

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

Manager responsibilities

Managers (general and financial) must ensure that all employees are aware of and comply with this policy.

Employee responsibilities

Each employee must ensure that he or she adheres to the content of if any aspect of this policy is unclear or needs clarification, such employee should obtain clarity in this regard from management.

2.6. TOPICS COVERED IN THIS POLICY

- End User Devices: This section details requirements regarding the use of any end user device that is used to access the company's networks, systems and data. The company owned end user devices (company end user device) and non-company owned end user device (personally owned devices). References to "end user device" will include both company owned and non-company owned end user devices.
- Personally Owned Devices: This section details requirements regarding the use of any end user owned device that is used to access the company's networks, systems and data.
- Use of Company IT facilities: This section details the company's requirements in terms of the use that employees and other people make of the company's IT facilities.
- Internet ,E-mail Usage and Social Networking usage: In order to protect the company and ensure the optimum utilisation of company communications facilities this section details policy regarding the use of E-mail, Social Networking and any Internet facilities accessed via facilities provided by the company.
- Social media in a private capacity: this section details personal conduct when using social media in a private capacity.
- Malicious Software Protection: The Company's facilities data and systems need to be protected from Malicious Software of all types. The regulations that need to be adhered to by the users are contained in this section.
- User Accounts and Passwords: This section details the behavior and conduct of all people who have access to the company's networks.
- Physical security: This section details the manner in which any equipment containing company data is protected from physical loss or damage.
- Software copyright and license agreements: The section details the rules that must be applied in the company in terms of software applications and licenses.
- Mobile and Home Computing Use: This section details the requirements of the company in terms of the use of mobile devices that are company owned and personally owned devices used to access the company network.
- Protection of Personal Information policy: This section is a set of guidelines and procedures put in place by the company to ensure the responsible and lawful handling of personal information it collects.

3. POLICY DETAIL

3.1. Company owned End User Device Usage

Access and use of company owned end user devices is provided to employees for the benefit of the company and its business. Access to the company owned an end user device is a privilege and such access is entirely at the discretion of the Management or specific delegates. Employees are able to connect to a variety of business information resources by using a company owned end user device.
Due care needs to be taken by users to ensure that company end user devices are not used for illicit or unauthorised purposes.

This section of the policy applies to users of devices that can be used to access the company's resources including but not limited to:

- Desktop workstations.
- Laptop computers.
- PDA's and Smartphones.
- Cellular Phones of any type.
- Thin Client Terminals, collectively known as "end user devices".

The usage of the device includes both the use of the hardware and the software located on these devices.
This section of the policy applies to all end user devices that access or interacts with company data and information systems.

3.1.1. Acceptable use

Company employees and other authorised users may make use of the end user devices for the purpose of conducting the company's business.

3.1.2. Unacceptable use

Users must not use the end user device for purposes that are illegal, unethical, and which may be harmful to the company. Examples of what employees shall not do, include but are not limited to the following:

- **Secondary business use**: Conducting a personal business using the end user device.
- **Excessive use**: Excessive use of an end user device for personal use, which then interferes with business functions being performed by the device.
- **Personal software**: Loading of personal software (legal or illegal) onto the end user device without the prior permission of the Management or their specific delegates or the employee's relevant manager. This also includes games whether legal or illegal.

3.2. Personally Owned Devices

Under special circumstances employees and other users are allowed to connect personally owned devices to the IT resources or facilities of the company. This includes connections to desktop computers, laptop computers, network points etc. Special care has to be taken in connecting these devices to the company's networks as the company could be liable for any and all information contained on these devices. This is particularly important if this information or software is transferred into the company IT systems, or if this information is not fully legally held by the user.

The personally owned devices being referred to include but are not limited to:

- Computers of any kind (Laptop, desktop, PDA, etc).
- Storage Devices (Memory Sticks, USB Hard Drives, Music Players, Data recorders).
- Communications devices (Cellular Phones, Modems, 3G Modems).
- Storage Media (CD and DVD Disk).
- Personal mobile Wi-Fi Access devices.

Personal devices are any devices that are not owned by the company, regardless of where the actual ownership resides.

3.2.1. Requirements

The following requirements must be taken into consideration in the use of personally owned devices.

- Personally owned devices of any kind can only be connected to the company's networks after permission has been obtained from the IT Department or relevant manager.
- Confidential company data should not be loaded onto any device without there being a critical requirement for the data to be stored on the device and prior permission having been obtained.
- Portable devices can be used for backup of less sensitive information if absolutely required e.g. the user is offsite at a location where the backup to the company's networks is either impractical (due to large size, cost) or impossible (unavailability of connection to company's network).
- Portable storage devices should not be used for long term backups of the user's data. This should be done on the company's servers.
- Personal mobile Wi-Fi access points should not be utilized during normal working hours if company IT facilities are available.

3.2.2. In using a personal device for the purpose of accessing company systems and information special software may be loaded onto the device and a mobile device management system may be implemented centrally. With this system in place the company will be able to enforce certain security measures to be in place on the personal device before access is allowed. This includes the following, in addition to the normal requirements of company owned devices:

- Minimum Standards: The mobile device may need to have a minimum standard in terms of the version of the operating system prior to the device being allowed access.
- Antivirus Protection: The mobile device may need suitable antivirus and anti-malware software installed prior to being allowed access.
- Acceptable Configuration: The mobile device may need to have a configuration that is acceptable to the company prior to being allowed access.
- Password Protection: The entire device or company area may need the user to enter a password prior to being allowed access. This password could be required every time the user enters the company area on the device.
- Password Strength: The password strength could be centrally set to ensure that it complies with Astral Policy.
- Encryption: It may be possible for all company related information or all information in either native or removable storage on the device to be encrypted to specified minimum encryption strength.
- Remote Lock Phone: It may be possible for the company or the user to lock a phone thus making it inoperable.
- Wipe Data: It may be possible for either the company or the user to delete all company related information on the mobile device. It may also be possible for the user to choose to wipe the entire device (perform a factory reset).Each employee might have to sign a wipe waiver prior to accessing the company network authorising the company to wipe the mobile device when it is deemed necessary.

3.2.3 Unacceptable use

Users must not use the personal devices for purposes that are illegal, unethical or harmful to the company. Examples of this include the following:

- **Illegal Information**: Copying of unauthorised material onto the company's networks. The company would be liable if this information was found in the possession of the company. This includes the transfer of all types of Illegal Content.
- **Illegal and Harmful Programs**: Personal devices are not to be used for the transfer or loading of computer programs onto the company's IT resources, especially if this software is illegal or potentially harmful.
- **Pornographic Material**: Personal devices must not contain pornographic material if they are connected to the company's network, as this could result in material becoming available and could thus become available on the network. Breach of this policy is subject to company disciplinary procedure. This applies to all the content and actions, simulated or real, graphic or written detailed in Schedules 1, 2, 6, 7 and 11 of the Films and Publications Act 65 of 1996.

3.3. Use of Company IT Facilities

The company's IT facilities have been put into place for the benefit of the company and its business. Access to the IT resources and facilities is a privilege and such access is entirely at the discretion of the operations management or their specific delegates. Furthermore, access to the computing resources does not necessarily imply permission to use them; this permission needs to be granted. It is however understood that employees of the company, who have such permitted access may from time to time utilise certain part of the company's IT facilities for limited private use. Care should however be taken by the employees to ensure that the IT facilities are not abused, and at no time should private use hinder the operations of the business.

This policy applies to any IT facilities that are provided by the company, and to which the user has access. This includes:

- Printers.
- Scanners.
- Copiers.
- Server and Networked storage capacity.
- Server processing capacity.
- Server based applications e.g. SharePoint.

Company employees and other authorised users may only make use of the IT resources and facilities for the purpose of conducting the company's business.

Users of the company's IT facilities are encouraged to:

- Consider the environment and not print documents if not required, to attempt to print duplex (on both sides of the paper) if possible, or to print multiple pages in a single page in order to reduce the use of paper.
- Print out draft copies in draft mode if possible and print colour only when required (not for draft copies).
- Avoid storing multiple version of the same document either on the server or workstation based storage, unless needed for business reasons.

3.3.1. Unacceptable use

Employees must not use the IT resources and facilities for purposes that are illegal, unethical or harmful to the company.

Examples of what employees shall not do include:

- **Secondary business activities**: Use any company resources or facilities for performing any business activities not related to the company's business.
- **Private use**: Excessively use company resources or facilities for personal use.

3.4. Internet, E-mail usage and Social Networking

The Internet is a large, publicly accessible network of networks that has millions of connected users and organisations world-wide. The Internet is the base for the provision and search for information, for the transfer of E-mail messages outside the company, and the provision of collaboration services such as instant messaging, news groups, chat rooms, social networking etc.
Access to the Internet, social networking sites and e-mail is provided to employees for the benefit of the company and its business. Access to the Internet, e-mail and social networking sites is a privilege and such access is entirely at the discretion of the operations management or their specific delegates. Employees are able to connect to a variety of business information resources around the world, through the Internet. Internet access through the group company network is limited to group company employees and others that the group company may authorise.
Conversely, the Internet 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 interests the following policy has been established for using the Internet, e-mail and social networking:

The Internet, e-mail and social networking facilities provided by the company are primarily intended for official business usage and to enhance the company's business. Private and personal use, in moderation, will be tolerated, subject to the rules detailed in this policy. The company will not accept any liability regarding the use of the Internet or e-mail facilities and social networking sites when used for private use, **and the employee hereby indemnifies the company against any such liability.**
E-mail users need to clearly understand that the use of electronic communications may cause the company to be held liable for legal liability arising through or caused by such use.
The company will manage and monitor E-mail to allow for the most productive use of IT resources.
The company has the right to limit the size of incoming and outgoing e-mail messages and attachments, downloads and other files and may block and delete e-mail messages, downloads, attachments or other files that are larger than the set maximum size. The company also reserves the right to block any type of message that is deemed not to be in the best interests of the company's business, e.g. download or upload of music files and/or images.

3.4.1. Acceptable use

Company employees and other authorised users may access the Internet, E-mail and social networking sites through the company's network for the purpose of conducting the company's business. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner

Examples of acceptable use of E-mail include:

- Using e-mail for business contacts and correspondence.
- Utilising the Internet, including e-mail, as a tool to advance the business objectives of the company.
- Limit the size of message sent via E-mail and avoid the download of large files from the Internet, especially during working hours. This is to prevent overloading of the electronic communication system resources.
- Not altering the contents of the original e-mail when forwarding e-mail or replying to e-mail. If the content needs to be changed, then all changes must be clearly marked as such.
- Not deleting E-mail data or attachments if required for company business.

Examples of acceptable use of the Internet include:

- Using the Internet to obtain business information for company use from commercial or academic websites.
- Accessing databases for information as needed for company business.
- Generally searching the Internet directly for information useful in achieving the user's business objectives.

Examples of acceptable use of Social Networking:

- Group communications is allowed to use social networking sites for business purposes and objectives of the company.

3.4.2. Unacceptable use

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

Examples of unacceptable use include:

- **Unacceptable content**: Receive and fail to delete, store, download, print, distribute, send or access any content or material that is offensive, harassing, fraudulent, racist, illegal or obscene (including any form of pornography as defined by the company). All other policies which refer to content are also applicable and should be taken into consideration by the user.
- **Spam**: Participate in e-mail "chain letters" or unsolicited e-mail ("spam"), for example, e-mail messages containing instructions to forward the message to others where not for official or company business purpose.
- **Sending Unnecessary Information**: Send or forward joke e-mails, electronic greeting cards, Christmas cards, copyrighted music files (e.g. MP3), copyrighted video clips (not related to official business) and games that can negatively impact on the overall performance of the company's communication resources.
- **Incorrectly Representing Company**: Represent personal opinions as that of the company via e-mail or publication of unauthorised statements onto web sites, blogs, wiki's, bulletin boards, discussion areas or newsgroups, etc. All other Astral Policies regarding the transfer of confidential business information to unauthorised parties needs to be taken into consideration.
- **Modifying E-mail Messages**: Modify an e-mail message and forwarding or replying therewith without noting the changes, i.e. deletions, removal of recipients or modification of content.

- **Masking Sender Information**: Send, reply to or forward e-mail messages or other electronic communications which hide the identity of the sender or represents the sender as someone else.
- **Fraud**: Use information, e-mail, files, downloads or data to commit fraud or any other criminal offence/s.
- **Secondary Business**: Conduct a personal business using company resources.
- **Disclosure of Confidential Information**: Transmit confidential information to any person not authorised to receive it.
- **Harming others**: Conduct any form of a campaign that may be considered as damaging against fellow employee/s or any third party by e-mail or by any other electronic means.
- **Modem use**: Use a peripheral communications device (3G Modem) whilst connected to the company's internal network. Under no circumstances is any modem allowed to be used when a workstation or laptop is connected directly to the company's network, thereby bypassing existing security mechanisms.
- **Obtaining restricted information**: Obtain or use copyrighted or restricted information to which the user does not have a right to obtain or use.
- **Abuse of the IT facilities**: Make unreasonable use of the Company's IT facilities in a manner which amounts to the abuse of the company's IT facilities.
- **Cautionary use**: Employees must exercise caution when using public, internet communication platforms to transfer information.

3.4.3. E-mail identification & disclaimer notice

To ensure that an e-mail message is properly identified apart from the sender's e-mail address it is compulsory that the sender places an e-mail signature and link to a separate disclaimer notice on the company's website at the foot of each individual e-mail message. The approved disclaimer is available from the group's various IT managers and it will be their responsibility to ensure that it is loaded onto all e-mail users' computers.

3.4.4. Monitoring

With due regard to the Constitution of the Republic of South Africa and the Regulation of Interception of Communications Act and Provision of Communications-Related Information Act, in order for the company to effectively manage its electronic communication resources the company reserves the right to;

- Intercept, monitor, block, delete, read and act upon any incoming or outgoing direct and indirect communications including but not limited to e-mail messages addressed to or originating from the employee. This includes all E-mail messages; even personal E-mails sent or received using the company's facilities.
- Intercept, monitor, read and act upon the employee's Internet browsing habits, including the user's history files, web sites visited, files downloaded and stored by the user; and
- Intercept, monitor, block, delete, read and act upon any file, in whatever format, stored by an employee on any computer or other facilities of the company.

The company will respect the employee's right to privacy as far as is reasonably possible, subject to the protection of the company's rights and interest in and to its business.

3.5 Social media in a private capacity

3.5.1 Confidential information

It is acceptable to talk about work and have a dialog with the community. Publishing confidential information about the Astral Group is however unacceptable. Confidential information is defined in the Standard Terms of Employment for all employees and includes, without limitation of the generality of this term, unpublished financial information, details of current projects, future product ship dates, research, and trade secrets. Respect the wishes of customers regarding the confidentiality of current projects. Be mindful of the competitiveness of our industries.

3.5.2 Protect your own privacy

Privacy settings that limit others from seeing your information that is personal should be set. Be mindful of posting information that you would not want the public to see.

3.5.3 Respect Astral and its employees

Do not embarrass the Astral Group, our customers, or your co-workers in any way. The public in general, and the Astral group's employees and customers, reflect a diverse set of customs, values and points of view. Do not state anything contradictory or in conflict with the Astral Group websites or official Astral Group documents. This includes not only the obvious (no ethnic slurs, offensive comments, defamatory comments, personal insults, obscenity, etc.) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory - such as politics and religion. Use best judgment and be sure to make it clear that any views and opinions expressed are yours alone and do not represent the official view of the Astral Group.

3.5.4 Protect Astral Group customers, business partners and suppliers

Customers, partners or suppliers should not be cited or obviously referenced without their approval. Never identify a customer, partner or supplier by name without permission and never discuss confidential details of a customer engagement. It is acceptable to discuss general details about kinds of projects and to use non-identifying pseudonyms for a customer (e.g., Customer 123) as long as the information provided does not violate any non-disclosure agreements that may be in place with the customer or make it easy for someone to identify the customer.

3.5.5 Controversial Issues

If you see misrepresentations made about the Astral Group or brands in the media, you may point this out to management who are better equipped to handle these issues.

3.5.6 Time spent

Please be cognisant of the amount of time spent on social media platforms. Personal social media use should not interfere with your job or commitments to customers.

3.5.7 Disclaimers

Social media users and bloggers who identify themselves as employees of the Astral Group should include a prominent disclaimer saying that they're not speaking officially on behalf of the Group.

3.5.8 Enforcement

Violations of this section and other Astral policies relating to the use of e-mail and social networks and social media will be subject to disciplinary action, which may give rise to dismissal in cases of serious misconduct.

3.6. Malicious Software Protection

Malicious software consists of programs such as viruses, trojan horses, spyware etc. This type of software is designed to make unauthorised changes to programs and data, or gather information and passwords from a person's computer or send messages from a person's E-mail system pretending to be that person. Viruses can cause destruction of corporate resources, loss of confidential data and disabling of communications facilities. It is important to know that malicious software is much easier to prevent than to cure. Defenses against malicious software include protection against unauthorised access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

Employees shall therefore;

- **Not knowingly introduce software**: Not knowingly introduce malicious software into end user devices.
- **Not deactivate antivirus**: Not deactivate the antivirus scanning engine on the end user device.
- **Not update antivirus**: Ensure that the antivirus signatures and engine is updated within one week of updates becoming available, especially if working offsite.
- **Not program updates**: Ensure that the Windows and other program patches are applied as required. A substantial part of these are security patches.
- **Not running programs**: Avoid running any programs or opening documents that have not been obtained from a reliable and trusted source. Even software and documents received from a trusted source should be reconfirmed with the sender since the software of program may have been sent by a virus or other malicious code that infected their system.

3.7. User accounts and passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorised employees have access to any data. This access will be restricted to only those capabilities that are appropriate to each employee's job duties.
The protection of all data and systems that the user has access to is based on the username and password of the individual. Persons who obtain access to someone's username and password will most likely have access to all the systems and data that the user has access to. This access may not only be from within the company's premises but also from outside the premises and even from the Internet depending on how the systems have been configured.
Users need to take special care in the choice and the use of their passwords. Simple passwords can be easily guessed by others. Passwords written down and stored with the computer can be used by others. A password can also become known to people when you type it in.

Each employee shall:

- **Responsibility**: Be responsible for all computer transactions that are made with his/her User ID (username) and password.
- **Password confidentiality**: Not share logon usernames or disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded or kept where they might be easily obtained.
- **Password complexity**: Use passwords that will not be easily guessed by others. Passwords should not consist of the personal details of the user e.g. spouses name, children's name, residential area.
  - Password must be eight or more characters long.
  - Password must contain the following:
    - ♣ Uppercase characters A-Z
    - ♣ Lowercase characters a-z
    - ♣ Digits 0-9
    - ♣ Special characters (!, $, #, %, etc.)
  - Password must be changed every 30 days.
  - Restrict users from reusing their last 24 passwords.
  - Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
  - Passwords must not contain months or days.

3.8 Physical security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, fraud, unauthorised access, and environmental hazards. Care must be taken to safeguard the electronic equipment assigned to employees. Employees who neglect this duty will be accountable for any loss or damage that may result.

An employee shall ensure that;

- **Secure storage of data**: Portable storage media is stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be adequately secured.
- **Secure storage of data**: Any storage media is kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- **Hazardous substances**: Other hazards to hardware such as food, smoke, liquids, high or low humidity and extreme heat or cold are avoided.
- **Changes to equipment**: No equipment installations, disconnection, modifications, and relocations undertaken without the permission of the Management .
- **Taking equipment offsite**: All users who are allocated laptop computers as part of their job role need to sign a consent form regarding use and safekeeping of the computer. Aside from this no equipment is to be removed out of the office without the informed consent of their department manager and/or MIS manager. Informed consent means that the manager knows what equipment is leaving, what data is on it and for what purpose it will be used.
- **Unauthorized equipment**: Under no circumstance connect any other equipment to the group company's network without prior, written approval from Management or a designated person.
- **Protection against Theft** - In case of theft of company owned computer equipment the individual responsible for the equipment will be liable for a co-payment of 50% of the original cost price of the equipment if such an individual has been found **negligent** in securing the equipment.
  Securing of computer equipment will also include the securing of equipment in vehicles, during travel and also when the vehicle is parked.
  Negligence will also include not ensuring that a vehicle is locked including instances where signal jamming equipment has been utilised to gain access to the vehicle. (Should equipment be stolen from a vehicle as a result of the signal jamming equipment the user will be seen to have been negligent.)
- **Due care as custodian of company asset –** All user should take the necessary steps to ensure that the company assets are not damaged. e.g. protective carry case and safely stored.
  In cases where it is found that an employee was **negligent** , the employee will personally be liable for the repair or replacement of the equipment.

3.9. 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. Employees shall therefore;

- **Copyright protection**: Not duplicate, copy or give to any unauthorised persons any copyrighted software.
- **Software installation**: No software should be installed unless authorised by Management who needs to verify that software is appropriately licensed. Only software that is licensed to or owned by the company is to be installed on company end user devices. Under no circumstances will any assistance/support be given on unauthorised or illegal products.
- **Downloaded software**: Not download and install software unless authorised by Management.
- **Unlicensed software: N**ot install any software for which the company does not have a sufficient number of licenses for the number of users.

3.10. Mobile and Home computing usage

Please note that this section of the policy applies to any employee with a company owned laptop, tablet or equivalent mobile device used to access the company's network or information resources whilst travelling to or from home or any other location. Employees with personally owned devices should however take due note of the items listed below in the best interests of the company. Employees who carry and use mobile devices are at risk due to the mobile nature of these devices. Accordingly, employees should thus take due care to ensure that mobile devices are not lost or stolen, nor that data is accessed by unauthorized persons. Employees thus need to be vigilant to the environment in which they are working in and concerned for the safety of the mobile device.

Employees shall therefore ensure the following:

- **Password protection**: Ensure that access to information contained on the mobile device will be protected by a minimum of a password into the operating system and screen savers. Additional access control through the device's BIOS or hardware levels are encouraged. This needs to be enabled by the IT department.
- **Encryption**: Where possible ensure that encryption for business related information is put into place by means of the device's operating system or any other similar application. This needs to be enabled by the IT department.
- **Unauthorized users:** Ensure that under no circumstances any unauthorised user is allowed to use the mobile device. This includes lending the device or handing over physical possession of the device to an unauthorised party.
- **Secure communications**: Ensure that when the company's network is accessed from home or during a business trip that the necessary security software that will establish secure communication to the company's security systems is utilised.
- **Foreign travel:** Understand that when travelling abroad all communications can be and frequently are intercepted and recorded.
- **Reading screens**: Take note that when travelling, especially in aircraft, buses or any other public transport, that external parties could easily read information off screens. Necessary caution should be exercised when working on company related information in public or non-company areas.
- **Hand luggage**: Ensure when travelling by aircraft, bus or any other means of mass or public transport, that the device is carried as hand luggage and not checked in. This will prevent damage to the device or the theft thereof.
- **Hotel security**: Ensure that when staying in hotels to make certain that the device is locked in a hotel safe and not left unattended in the hotel room.
- **Device identification**: Make sure that the carry case and device is clearly identified. Other methods of identifying the device, for example engraving or fluorescent marking are encouraged.
- **Storage in car**: Make sure that if you are unable to take the device with you it is locked away from sight when left in a vehicle, for example in the vehicle's boot – including when travelling. When parking anywhere, employees must ensure that the vehicle is actually locked before leaving it and that the use of a blocking signal device has not prevented the vehicle from being locked. This does not include extended periods such as overnight, when the device shall be stored securely outside the vehicle. The individual responsible for the equipment will be liable for a co-payment of 50% of the original cost price of the equipment if such an individual has been found **negligent** in securing the equipment

- **Device locking**: Ensure that the device is securely locked with the supplied security cable when working at a desk outside of the company.
- **Data backups**: Make backups of crucial files on the device at least weekly and store these separately from the device on the company's server.
- **Passwords security**: Do not save any passwords or access codes anywhere on the device. This includes taping notes onto the device or keeping them inside the carry case of the device.
- **Environmental protection:** Not leave the device in direct sunlight or where it is exposed to any other environmental hazards such as dust, liquids, chemicals and food.
- **Cleaning:** Not use household chemicals or water to clean the device – use a dust cloth.
- **Physical protection:** Not drop or knock the device and perform a regular check on the condition of the strap of the carry case and the carry case itself.
- **Theft reporting:** In the event of a mobile device being stolen, immediately report the theft to Management to arrange for all security access to be suspended.

4. Protection of Personal Information Policy

Employees and other persons acting on behalf of the organisation will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

Employees and other persons acting on behalf of the organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects. Employees and other persons acting on behalf of the organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties. Employees and other persons acting on behalf of the organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the organisation will only process personal information where:

- the data subject, or a competent person where the data subject is a child, consents to the processing; or the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- the processing complies with an obligation imposed by law on the responsible party; or
- the processing protects a legitimate interest of the data subject; or
- the processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject: - clearly understands why and for what purpose his, her or its personal information is being collected; and - has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information. Employees and other persons acting on behalf of the organisation will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information. Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the organisation will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed. Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the organisation will under no circumstances:

- process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's dedicated server.
- share personal information informally. In particular, personal information should never be sent by e-mail, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- transfer personal information outside of South Africa without the express permission from the Information Officer.

Employees and other persons acting on behalf of the organisation are responsible for:

- keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the organisation, with the sending or sharing of personal information to or with authorised external persons.
- ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- ensuring that where personal information is stored on removable storage medias such as external drivesand that these are kept locked away securely when not being used.
- ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.

- taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via e-mail. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- undergoing POPI Awareness training from time to time.

Where an employee, or a person acting on behalf of the organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer

5. Acknowledgement of End User Policy

Each employee assigned a desktop or laptop computer or a mobile device, workstation or network account needs to sign the following acknowledgement form and return it to Management who will then ensure that it is included in the relevant employee's personnel file.

Acknowledgement of Astral IT Policy

Procedure:

1. Read the “Astral Group IT Policy”. If there are any aspects regarding this policy that are unclear please consult with your Manager.
2. Sign in full and complete the details in the spaces provided below.
3. Return this acknowledgement form to your Manager for record keeping purposes.

Signature

By signing below, I agree to the following terms:

- I have received and read a copy of the "*Astral IT Policy”* and understand the same.
- I understand and agree that any computer, software, and storage media provided to me by [Operation] contains proprietary and confidential information about [Operation] and its business and remains the property of the company at all times.
- I agree that I shall not copy, duplicate (except for purposes as part of my job here at [Operation]), or otherwise disclose, or allow anyone else to copy or duplicate any of the information or software on any computers, software or storage media provided to me.
- I agree that, if I leave [Operation] for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, storage media or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.
- I agree to abide by the terms set out in the “*Astral IT Policy*” and to be bound thereby. In particular, I understand and accept that in appropriate circumstances Astral may monitor and intercept the information, data and e-mail on my computer, and I hereby grant my consent for such monitoring and interception in terms of section 5 and 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002.
- I understand and agree that failure on my part to comply with the terms as set out in the “*Astral IT Policy*” and this acknowledgement form may result in disciplinary action being taken against me.

Employee signature: _____

Employee name: _____

Department: _____ **Date:** _____