WOLFPACK POPI INTERNAL APPROVAL DOCUMENT

- POPI recognises a person's constitutional right to privacy and therefore the protection of personal information is vital for the sustainability and growth of the business.
- For example: This means you can not give out a person's personal information such as a telephone (cell number) or personal address out to another person, without that particular party's consent.

1. General Processing of Personal Information:

Purpose of this policy is merely to incorporate the requirements of the Protection of Personal Information Act into the everyday operations of the business to ensure compliance. This requires you to inform a person when you are collecting their personal information and obtain their consent (have them sign for it). Persons in the office environment – to keep records of personal information accurate and up to date.

- Every employee will be required to comply with this Act and policies.
- The point of contact for requests, disclosures, questions, complaints and any other enquiry relating to the handling, collection, processing or re-identifying of personal information shall be directed to the Information Officer.
- Information Officer: Mr Justin Anley
- Violation of these policies may lead to disciplinary action/hearings and may lead to dismissal.

2. Duties and Responsibilities of the Information Officer:

- Encourage compliance with this act for the lawful processing of personal information.

- Working closely with the Regulator when investigations are conducted into the business as to the processing of personal information.
- Ensuring compliance with these policies.

3. Prohibition of Special Personal Information:

- You may not process personal information regarding a person's religious beliefs, race, trade union membership, political persuasion, health or sex life or biometric information unless: information has deliberately been made public by the data subject, the processing is carried out with the consent of that person, or there is an obligation by law or public law duty to collect such information, or collection is for a research or statistical purpose.

4. Direct Marketing by Means of Unsolicited Electronic Communications:

- Sending out bundle emails to or approaching someone with the intention of marketing products here. May only approach a person once, if that person says no, do not approach them again.
- If you do approach someone with the intention of marketing, your details must be clear to such a person, and include your contact details so that person may get hold of you regarding your communications.

5. Acceptable Use Policy:

- Acceptable use and security of the business internet facilities.
- Software, hardware and computer networks are the property of the business and it therefore reserves the right to monitor these and to carry regular checks on the system.

- Electronic files created, sent, received, or stored on Information resources owned, leased, administered or otherwise under the control of the business are the property of the business and employee use of these files are not private and not personal.
- The Information officer may access these files at any time without the knowledge of the user/owner.
- Business management reserves the right to monitor and log all employee use of the business's information resources without prior notice.
- Any security threats, unexpected software or system behaviour/malfunction must immediately be reported to management.
- Do not try to access anything you do not have authority for.
- Do not share your account passwords, any PIN numbers, security tokens or any other information/devices which are used for identification or authorisation purposes.
- Do not make unauthorised copies of any software owned by the business.
- In particular, the business internet facilities may not be used for the following:
    - Downloading, transmission and possession of any pornographic or sexually explicit materials;
    - Transmitting defamatory, slanderous, threatening and abusive messages;
    - Political or religious statements;
    - Foul language or harassing statements;
    - Unauthorized attempts to bypass security systems of the business;
    - Forwarding chain letters or junk emails;

    - Infringing on the right to privacy of other employees on the email system;
    - Playing computer games or taking part in entertainment during working hours;
    - Any activity which could harm the good name and reputation of the business.
- Any employee may at any time anonymously report policy violations to the Information Officer.

6. Email Policy:

- Business email system must be used primarily for business purposes;
- The Business reserves the right to monitor, inspect, copy, review, and store any and all employee email use at any time and without prior notice;
- The business reserves the right to disclose email information and images to regulators, courts, law enforcement agencies and other third parties without the employee's consent;
- Employees are prohibited from using emails to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.
- Unless authorized to do so, employees are prohibited from using emails to transmit confidential information to outside parties.
- Confidential information includes: client lists, credit card numbers, id numbers, employee performance reviews, salary details, trade secrets, passwords and information that could embarrass the business and its employees if the information were to be disclosed to the public.
- All messages communicated on the Business Internet and email system must contain the employee's name. No email

or any other form of electronic communication may be sent which hides the identity of the sender or represents the sender as someone else. Therefore all emails must contain the email signature of the sender.

- Please ensure that you have an email disclaimer at the bottom of all your emails.

7. Handheld and Mobile Device Policy:

- Ensure that all use of business phones are for business purposes only;
- If you feel required to download an app for some reason, bring this to the attention of your Information officer who will guide you accordingly.

8. Access Control Policy:

- User accounts will have access only to what the user is required to have access to;
- All passwords must be constructed using the following: mixture of letters, numbers and special characters.
- You are responsible for your password; do not divulge this to anyone without the prior authorisation of the information officer.

9. Physical Security Policy:

- Access to the premises
- Do not leave personal information in public areas unattended;
- If you are leaving your computer desk and same is situated in a public area, rather log out than leaving personal information open and unattended.

10. Anti-Virus Policy:

- Ensure that anti-virus programmes are updated regularly;
- Do not attempt to remove a virus yourself, rather disconnect your PC from the business network and stop using same immediately. Speak to your Information Officer to obtain IT to sort out the problem.
- If you receive an email from an unknown sender and attachment seems dodgy, rather forward it to IT than opening it yourself.

11. Data Retention Policy:

- This policy applies to all documents which are collected, processed or stored by the Business and includes but is not limited to documents in paper and electronic format, for example, email, web and text files, PDF documents, etc.
- Check the retention period with the Information Officer;
- Certain documentation must be kept for a certain period, therefore do not attempt to store information by yourself, even something you may deem to be scrap.

12. Data Destruction Policy:

- All forms of computer equipment, digital storage media and printed or handwritten material must be displosed of securely when no longer required.
- Under no circumstances should paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.
- Data should be removed in such a way that it is not virtually retrievable;
- Employees must ensure that all paper documents that should be disposed of, be shredded locally within the department

and then be recycled. Where local shredding is not possible, bulk quantities of restricted paper waste must be held in waste sacks. These will be collected and disposed of by an employee instructed to do so by the information officer.

13. Risk Management Policy:

- Identify risks in the day to day operations of the business.
- These hazards include, but are not limited to, the physical work environment, the equipment, materials and substances used, the work tasks and how they are performed.
- NB: Know which hazards you are exposed to on a daily basis and the precautions you need to take to minimize the potential damage.

14. Information Classification Policy:

- All information entrusted to the business by a third party must be classified and protected accordingly.
- Look at what is Unclassified Public, Proprietary and Client Confidential Data.
- When you have a Confidentiality Agreement regarding information, do not give out that information to anyone and be guided by your information officer accordingly.

15. Disaster Recovery Policy:

- When an information breach occurs and the Information Officer sets up Policies (or steps) to be taken to ensure extra security) please ensure that you comply with same and that you keep your information officer informed on your responsibilities regarding protection of personal information.

16. Cookies Policy:

- We use cookies responsibly on this site to provide a better user experience. Cookies are used to recognise and count

the number of visitors and see how visitors move around the site to improve the way our website works.