BAYPORT FINANCIAL SERVICES 2010 (PTY) LTD

and its affiliates

(Hereinafter referred to as “Bayport” or “the Company”)

Protection of Personal Information Act (POPIA) PRIVACY POLICY

Table of Content

1. Overview

This Policy describes the way that Bayport Financial Services (hereinafter referred to as *"Bayport"*), will meet its legal obligations and requirements concerning data protection. The requirements within this policy are primarily based upon the Protection of Personal Information Act, No 4 of 2013 (hereinafter referred to as *"POPIA"*), as that is the key piece of legislation covering data protection.

A POPIA Privacy Policy must be developed to ensure that Bayport as a responsible party, complies with the provisions of POPIA. This policy must detail the measures that Bayport is taking to proactively ensure compliance with the provisions of POPIA.

2. Statement of Purpose

This document has been prepared to provide a framework for the safeguarding of Bayport's customers' (both internal and external), contracting third parties, and its employees' personal information, compliance with relevant legislation and to serve as a reference document for internal quality control processes.

The objectives defined in this document may in certain cases conflict with other business objectives (such as improved efficiency and the reduction of costs). Management has examined these conflicts and resolved that the controls set out in this policy are required to manage the risks to Bayport. The responsibility to ensure the protection of personal information is not limited to the IT or compliance departments but requires the co-operation of the business unit and every employee. This policy has accordingly been written with the following goals in mind:

a) To guide the establishment and implementation of the POPIA project; and
b) To facilitate the establishment of policies, processes and business rules to ensure the protection of personal information as envisaged in POPIA.

3. Definitions

3.1. **''data subject''** means the person to whom the personal information relates;

3.2. **"electronic communication"** means any communication of information by electronic means;

3.3. **"electronic communications systems"** means all systems used by Bayport that enable electronic communications, including (without limitation) the Internet, voice mail, electronic mail, digital communication (e.g. WhatsApp and SMS), social media and facsimiles;

3.4. **"employee"**, refers to a part-time or full-time employee of Bayport;

3.5. **"incident"** means any problem, malfunction, breach or suspected breach of information or the compromise of an information system;

3.6. **"information"** means representations of information in any form generated, sent, received or stored and includes:

3.6.1. voice, where the voice is used in an automated transaction; and

3.6.2. photo, where a hard copy or digital photograph is used in an automated transaction; and

3.6.3. video, where the video is used in an automated transaction; and

3.6.4. A stored record.

3.7. **"information system"** means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes electronic communications systems;

3.8. **''operator''** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

3.9. **"personal information"** has the meaning given to it in POPI, being information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

3.9.1. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

3.9.2. information relating to the education or the medical, financial, criminal or employment history of the person;

3.9.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

3.9.4. the biometric information of the person;

3.9.5. the personal opinions, views or preferences of the person;

3.9.6. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

3.9.7. the views or opinions of another individual about the person; and

3.9.8. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

3.10. **"policy"** refers to the Bayport POPIA Privacy Policy;

3.11. **''processing''** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

3.11.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

3.11.2. dissemination by means of transmission, distribution or making available in any other form; or

3.11.3. merging, linking, as well as restriction, degradation, erasure or destruction of information;

3.12. **''responsible party''** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

3.13. **"Special Personal Information''** is a subcategory of personal information given the highly sensitive nature of such information. It includes information concerning a child and personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, DNA, sexual life or criminal behaviour of a data subject.

4. Categories of Data Subjects and their Personal Information

Bayport may possess records relating to suppliers, shareholders, partners, contractors, service providers, employees and customers;

Entity Type	Personal and/or Special Information Processed
Customers: Natural Persons	Name, surname, ID number, date of birth, physical and postal address, telephone numbers, email address, salary information, gender, marital status, employment information, bank details, next of kin details, tax information, financial records and financial history, Union membership.
Partners: Juristic Persons / Entities / Contracted Service Providers	Names of contact persons; the name of the legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax-related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Employees, Contractors/ Contracted Service Providers and Directors	Name, surname, ID number, physical address, postal address, email address, date of birth, salary information, race, gender, marital status, employer information, telephone numbers, bank details, next of kin, tax information, financial records, pregnancy; colour, age; language; education information; financial information; employment history; opinions; criminal record; wellness information; medical history

5. Categories of Recipients for Processing the Personal Information

Bayport may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. Bayport may supply the Personal Information to any party to whom Bayport may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to customers;
- Conducting due diligence checks;
- Administration of Medical Aid and Pension Schemes.

6. Channels Used for the Collection of Information

6.1. General:

The Bayport Information Security Policy sets the methodology for preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of any information.

Bayport collects Information in various ways e.g., directly from individuals (for example, when purchasing a financial or credit product, registering an account, using a product, or signing up for a newsletter), from employers, publicly available information, through cookies, and/or similar technology.

Bayport must inform Data Subjects which information they are legally required to provide to Bayport, and which information is optional. With the Data Subject's consent, Bayport may supplement the information with other information received from other companies and/or organizations such as credit bureaux or the South African Revenue Services (SARS) to enable Bayport to render suitable and proper services to Data Subjects.

6.2. User Supplied Information:

The Data Subject may be required to provide some personal information, for example, his/her name, address, phone number, email address, banking details (*if applicable*), and/or certain additional categories of information as a result of using/receiving credit and/or financial services, purchasing credit and/or financial products, and using websites and related services. Bayport will keep this information in an appropriate database for future reference, as needed.

6.3. Usage and Web server logs

Bayport may track information about a Data Subject's usage and visits on the Bayport website. This information may be stored in usage or web server logs, which are records of the activities on Bayport's services, products and/or sites. Bayport's servers automatically capture and save such Information electronically. Some examples of the Information that may be collected include the Data Subjects:

- Unique Internet protocol address;
- Name of the Data Subject's unique Internet Service Provider
- The city, province, and country from which a Data Subject accesses Bayport's website
- The kind of browser or computer used;
- The number of links clicked within the site;
- The date and time of visits to the site;
- The web page from which the Data Subject arrived on Bayport's site;
- The pages viewed on the site;
- Certain searches/queries conducted on the site via Bayport's services, products and/or websites.
- The information collected in usage or web server logs helps Bayport to administer the services, products and sites, analyse its usage, protect the product and/or website and content from inappropriate use and improve the user's experience.

6.4. Cookies

To offer and provide a customized and personal service through Bayport's products and websites, Bayport may use cookies to store and help track information about the Data Subject.

A cookie is a small text file sent to the Data Subject's device that the Bayport uses to store limited information about the Data Subject's use of the services, products or website. Bayport uses cookies to provide the Data Subject with certain functionality (such as to enable access to secure log-in areas and to save the Data Subject having to re-enter information into the product, services or website forms) and to personalize Bayport's services, products or website content. Without cookies, this functionality would be unavailable.

7. POPIA Compliance

7.1. Purpose and Application of the POPIA Compliance

7.1.1. Introduction

Bayport as a registered credit and authorized financial services provider is required to meet certain legislative requirements in terms of the National Credit Act, 2008 (hereinafter referred to as *"NCA"*) and the Financial Advisory and Intermediary Services Act, 2002 (hereinafter referred to as *"FAIS Act"*). These acts provide for the protection of personal information of Clients and POPIA provides for 8 Data Protection Information principles to comply with to ensure the protection of all data that relates to companies, employees and clients. The Promotion of Access to Information Act, 2000 (hereinafter referred to as *"PAIA"*) provides for access to such information and in which instances it may be refused.

7.1.2. Purpose

Data privacy and protection is important to Bayport and this policy and framework set out the POPIA principles in line with existing FAIS and NCA requirements to ensure the safekeeping of all Data processed by Bayport and associated Persons/ Employees/ Parties (*as applicable*). This document thus applies to all Data obtained via partners, 3rd parties, products, services, websites and events operated by Bayport or by any other means.

7.1.3. Embedment of 8 POPIA Principles

7.1.3.1. Principle 1 - Accountability:

Bayport will ensure that technology, structures, processes, procedures, roles and responsibilities will be put in place, in addition to the current controls, to create an environment where Personal Information is processed lawfully. This applies from the moment of collection to any and all subsequent forms of processing.

Bayport has appointed an Information Officer who is a senior person in the organisation and is part of the Executive Committee. Bayport has also resolved to appoint one or more Deputy Information Officer(s), who, together with the Information Officer, will be responsible for ensuring that Bayport has been properly informed and trained on ensuring the safekeeping and protection of Information within the organisation and that the required processes are implemented to ensure compliance. The Information Officer and his Deputy(ies) can be contacted on the below details;

- Information Officer
  - Name of Officer: Arthur Hlubi
  - Contact Number of the Information Officer: 0872874000

- Deputy Information Officers
  - Name of Information Officer: Haydn Venter
  - Contact Number of the Information Officer: 0872874000
  - Email Address of the Information Officer and Deputy Information Officer/s: popia@bayport.co.za

Bayport will formulate and implement a governance framework that will give effect to the policy statements in this document.

7.1.3.2. Principle 2 - Processing Limitation:

When processing or further processing Personal Information, Bayport will ensure that it is done in a lawful and reasonable manner and does not knowingly infringe on the rights of the Data Subject.

Bayport will only process the minimal required information to provide the service or product to the Data Subject. No excessive information will be processed. To do this, all business units that process personal information within Bayport will define the personal information they deem necessary to perform activities specific to their functions and ensure that no personal information in excess of this is processed.

Bayport has interpreted POPIA to imply that consent does not have to be gained explicitly where processing Personal Information is necessary during the course of fulfilling a contractual or performance obligation. As interpreted, Bayport will process Personal Information when the following conditions are met:

a) It is necessary to deliver the service or product required by the data subject,
b) It is required to conclude a contract, adhere to the law, comply with an obligation or protect a legitimate interest of the data subject.
c) It is required to enforce the terms of the contract between the parties.

Bayport will allow for a Data Subject to object to the processing of their Personal Information or withdraw consent initially given. Bayport will ensure that this is done in the prescribed manner, on reasonable grounds relating to the Data Subject's situation.

If this results in Bayport not being reasonably able to comply with its contractual or performance obligations, Bayport will follow the standard, reasonable business processes to end the contractual relationship with the data subject. Bayport agrees that it will not process the personal information where the data subject has objected to same unless legally allowed to do so.

Personal Information will be collected directly from the data subject, unless:

a) Collection from other sources does not prejudice the data subject, or
b) It is already from a public record, or
c) The data subject consented to the collection of the information from another source, or

d) The collection from another source will not prejudice the legitimate interest of the data subject, or
e) Is not reasonably achievable, or
f) In compliance with an act.

7.1.3.3. Principle 3 - Purpose Specification

Bayport will collect personal information for a specific purpose which will be defined in relation to a function, or activity performed by Bayport. The purposes of the collection of personal information include the following:

a) Rendering suitable services such as the granting of credit agreements in line with the NCA, financial services in line with the FAIS Act (including the rendering of advice and intermediary services) and administrative services to Data Subjects;
b) Improving services and product offerings to Data Subjects;
c) Providing information and resources most relevant and helpful to Data Subjects;
d) Appointing suitable individuals/ companies to provide the said services/ products to Data Subjects.
e) Ensuring compliance with legislation that requires specific information to be collected as envisaged in the Bayport Data Retention Policy.
f) The enforcement of contract terms that exist between the Data subject and Bayport.

A process will be defined and developed to set out how a Data Subject will be made aware of the purpose for which their personal information was collected.

Bayport will not retain any personal information longer than is necessary to achieve the purpose for which it was collected, or subsequently processed unless

i. It is required by law: Bayport will undertake efforts to identify retention periods as stipulated in regulations and laws applicable to the business**;** or
ii. Bayport requires the record for lawful purposes related to its business interests, functions and/or activities: In the absence of a requirement by law, Bayport's functions will define purposes for retention of records for purposes related to that function

When the records are no longer required, Bayport will destroy and/or de-identify the personal information within a reasonable period of time. The process to destroy and/or de-identify personal information will be captured in the Bayport Data Retention and Destruction Policy.

7.1.3.4. Principle 4 - Further Processing Limitation

Where Bayport is required to further process the information, (such as where data is further processed for insurance claims purposes or analytical purposes for a report to rating agencies), this will be done in line with the original purpose for which it was collected. This extends to cases where further processing will result in a clear benefit to the data subject or a third party.

To assess whether further processing is allowed, consideration will be given to:

a) The contractual relationship between Bayport and the data subject,
b) The consequences of further processing for the data subject, and
c) The nature of the information collected.

Further processing will be considered lawful for Bayport if the information is derived in terms of the statements hereunder:

a) It is derived from a source within the public domain;
b) It is required to avoid prejudice, required for court proceedings or to adhere to the South African Revenue Services Act, 1997.
a) It is required as a matter of national security or to prevent a real or imminent threat to public health and safety or the data subject
b) For historical, statistical and research purposes and in a non-identifiable form.

7.1.3.5. Principle 5 - Information Quality

Reasonable, practical steps will be taken by Bayport to ensure that all information collected is accurate, complete, not misleading and up to date in accordance with the purpose for which it was collected. In line with internal Know Your Customer (KYC) procedures and standard background checks on all data subjects upon the establishment of a business relationship, as well as standard operating procedures within individual business units where the accuracy of the information on record is confirmed at every point of contact, after the establishment of a business relationship

7.1.3.6. Principle 6 - Openness

When Personal Information is collected, Bayport will take reasonable practical steps to make the Data Subject aware of:

a) The Personal Information about him/her that is being collected;
b) The purpose for which the Personal Information is collected;
c) Whether the information supplied is voluntary or mandatory;
d) The consequences of failure to provide the information;
e) Whether third parties are involved in processing the information; and
f) The data subject's rights as it pertains to:
    - Access to their Personal Information;
    - Their rights to object to processing;
    - Their right to lodge a complaint with the information regulator.

The said steps include but are not limited to the inclusion of details of the abovementioned aspects in relevant documentation issued to the customer as well as full terms and conditions available on the Bayport website.

Pursuant to the Openness Principle as per POPIA, Bayport will embed channels to make data subjects aware of the detail highlighted above, in existing, relevant business processes as follows:

a) Full and detailed Privacy Notice: Bayport public website;

b) Summarized Privacy Notice: Terms and conditions for policy wording;
c) Short Form Notices: In-bound and out-bound call centre scripts, letters and form footers.

7.1.3.7. Principle 7 - Security Safeguards

Bayport will implement appropriate security measures to safeguard and secure the Personal Information in its possession or under its control. It will undertake appropriate, reasonable technical and organizational measures to prevent:

a) Loss, damage or unauthorized destruction of Personal Information; and
b) Unlawful access to or processing of Personal Information.

Bayport will not disclose or share Information relating to any Data Subject unless;

a) It is specifically agreed with the Data Subject; it is already publicly available or in the interests of the public
b) It is required in terms of Law or;
c) If the Bayport believes in good faith that the law requires disclosure thereof.

Bayport stores Personal Information about Data Subjects in a restricted access server with appropriate monitoring and uses a variety of technical security measures to secure Personal Information, including intrusion detection and virus protection software.

Bayport will secure the integrity and confidentiality of Personal Information by taking reasonable practical steps to:

a) Identify foreseeable internal and external risks to Personal Information through the inclusion of privacy risk reviews in the organisation's risk management programme;
b) Establish and maintain appropriate safeguards against risk as monitored by the organisation's Information Technology Governance Risk department;
c) Ensure ongoing, continual updates of risk responses.

When Personal Information is processed on behalf of Bayport, the third party must process only:

a) With the knowledge or authorization of the responsible party;
b) Treat the Personal Information as confidential, unless required by law or in the course of performance of their duties;

Bayport will ensure, with written contracts between itself and its operators or co-responsible parties, to establish and maintain security safeguards as it applies to itself. Bayport's PAIA Manual (as required by PAIA), has been aligned with the provisions of POPIA and sets out the process for access by third parties to a Data Subject's Information kept by Bayport, and the instances in which it may be refused.

Bayport will embed a process where, in the instance(s) that there are reasonable grounds to believe that the personal information of a data subject that is processed by Bayport has been accessed, or acquired by any unauthorised

person, the regulator and the affected data subject(s) are notified as soon as reasonably possible.

Bayport will ensure that adequate detail is provided to the affected data subjects including, but not limited to, the following:

a) Possible consequences of the security compromise;
b) The measures that Bayport intends to take, or has taken to address the compromise;
c) Recommendation of any measures that the data subject can take to mitigate possible adverse effects of the compromise; and
d) If known to Bayport, the identity of the unauthorized person.

7.1.3.8. Principle 8 - Data Subject Participation

Bayport recognizes the rights of a data subject who has adequately validated their identity to gain access to their Personal Information.

Bayport will confirm, free of charge, whether or not Bayport holds Personal Information about the data subject. This process should be managed as part of the existing business-as-usual business processes.

In the case where the data subject requests a record or description of Personal Information held by Bayport, the data subject can download the Personal Information request form from the Bayport website and contact the Information Officer on the details provided above. Bayport will ensure that the detail requested is provided:

a) Within a reasonable time,
a) At a prescribed fee,
b) In a reasonable manner and format, and
c) In a form that is understandable.

To effectively manage Data Subject Participation, it will be managed via the Data Subject Access Management process. Any dispute or reasons for the non-supply of information will also be dealt with through this process.

A data subject may request Bayport to update, delete or correct information which is inaccurate, irrelevant, out of date, incomplete or obtained unlawfully by contacting the client services department on 087 287 4000. Bayport will take all reasonable steps to confirm the data subject's identity before making changes to the Information.

Where the deletion or change of the information will change decisions or the ability to fulfil contractual obligations to the data subject, the data subject should be informed of this and the resultant consequences should be clarified.

7.1.4. Additional POPIA Applications

7.1.4.1. Special Personal Information and Information of Children

Bayport will not process Special Personal Information and Information of Children unless:

a) The Processing is carried out with the data subject's consent, or in the case of children, with the prior consent of a competent and legally authorized person;
b) Processing is necessary for the establishment, exercise, defence of a right or Regulatory Requirement;
c) Processing is necessary to comply with international public law.

The Processing is for historical, statistical or research purposes to the extent that:

a) It serves a public interest and is necessary for the Purpose concerned; or
b) It appears to be impossible or would involve a disproportionate effort to ask for consent and enough guarantees are provided, to ensure that the Processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

7.1.4.2. Direct Marketing

Bayport will gain prior consent from the data subject in order to market directly to the data subject. This relates to all forms of electronic communication and channels for the purpose of direct marketing including the following:

a) Automatic calling machine
b) Facsimile machines
c) SMS, Telegraph or WhatsApp
d) Email

Bayport may approach a data subject to obtain their consent to market directly if they have not previously withheld consent.

In the instance that Bayport directly markets to a data subject who is a customer of Bayport, Bayport must ensure the following:

i. Contact details were obtained in the context of the sale of a Bayport product, or service;
ii. The purpose of the marketing is of Bayport's similar products or services;
iii. The data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, at the time the information was collected, or on the occasion of each communication if the data subject had not initially objected to such communication

If a data subject withdraws their consent for direct marketing Bayport must cease to market directly as per the Direct Marketing Policy.

7.1.4.3. Automated Decision Making

Bayport uses models that make automated decisions based on predefined parameters to conclude agreements with data subjects. Bayport will not make a decision that will subject a data subject to legal consequences or negatively affect him substantially based solely on the automated processing of information unless:

a) It is taken in connection with the conclusion or execution of a contract;
b) At the request of the data subject or measures have been taken to protect the data subject's legitimate interest;
c) It is governed by a law or code of conduct.

Bayport will ensure that measures are in place that ensure that:

a) The data subject's rights and legitimate interests are not infringed;
b) The data subject can request human intervention to discuss the decision or contest it; and
c) Where necessary, the logic of the automated decision-making mechanism used can be explained.

7.1.4.4. Transborder Information Flows

At times, Bayport transfers data containing Personal Information to third parties outside of the Republic for purposes of *inter alia* storage and reporting. In the instances that Bayport transfers this information, Bayport will ensure the following:

a) The third-party who is the recipient of the information is subject to a law, binding corporate rules and/or binding agreement which provides an adequate level of protection;
b) The data subject consents to such transfer;
c) The transfer is necessary for the performance of a contract between the data subject and Bayport;
d) The transfer is necessary for the conclusion, or performance of a contract concluded in the interest of the data subject between Bayport and the third party; or
e) The transfer is for the benefit of the data subject.

7.2. Policy Implementation Plan.

For Bayport to ensure compliance with the provisions of POPIA, several changes to business policies and processes must be implemented to ensure alignment with the provisions of POPIA. To ensure coordination of these efforts, a policy implementation plan must be formulated and implemented within the permitted timelines to ensure compliance. The following elements of this plan are noted and amendments to the plan will be managed and monitored through the life cycle of the plan.

7.2.1. Formalisation of the POPI Act compliance project

7.2.1.1. Identification and noting of relevant stakeholders

The responsibility of identification and noting of relevant stakeholders lies with the POPI Steerco which is tasked with the oversight of the policy implementation plan. The Project Manager must note said stakeholders and liaise with them periodically to evaluate the progress of their respective policy implementation efforts.

7.2.1.2. Noting of the Project Sponsor

In line with POPIA, the Information Officer is responsible for, amongst other things, ensuring that Bayport complies with the provisions of POPIA. As such, the Information Officer is the appropriate party to fulfil this role.

7.2.1.3. Noting of the Project Manager

The Deputy Information Officers are appointed as the POPIA Project Managers and are responsible for managing the policy implementation plan with oversight from the POPIA Steerco and the Project Sponsor.

7.2.1.4. High-level scope, timescale and budget

The Information Officer, in consultation with the project manager, relevant stakeholders and the respective governing body, must approve a high-level scope, timescale and requisite budget for the policy implementation plan.

7.2.2. POPIA Gap analysis

7.2.2.1. Interim and final targets for compliance with the POPI Act.

The Project Manager, through the appropriate channels, shall communicate the interim and final targets for compliance with POPIA. This information will be noted in the project plan wherein, several sub-projects will be noted and documented accordingly with their interim and final target dates.

7.2.2.2. Engagement methodology with stakeholders in the assessment

The Project Manager will, in consultation with the relevant stakeholders be the central point of contact and engagement on all matters about the policy implementation plan. As such, the Project Manager shall determine the appropriate engagement methodology with the stakeholders.

7.2.2.3. Approach to Gap Analysis

The Project Manager in consultation with the POPIA Steerco will determine the appropriate approach to GAP Analysis and will, in consultation with the relevant stakeholders, communicate with the governing body and Project Sponsor on the outcomes and recommendations to address the gaps.

7.2.2.4. Document Gap assessments for ongoing compliance monitoring

The Information Officer in consultation with the Deputy Information Officer/s, shall document or delegate the responsibility of documenting the Gap assessments for ongoing compliance.

7.2.3. Analysis of what and how Personal Information is processed

Bayport, through the development of a Data Library, shall analyse what information is held by Bayport and how this information is processed. This exercise shall;

a) Record types of information as per POPIA (e.g. CCTV, biometric)
b) Note aspects of record types, i.e. consent, purpose, source, storage, sharing, destruction and re-identification.
c) Consider user rights and user rights management

d) Conduct device and system vulnerability assessment (what the types of devices are where they are data stored – and which represent a security compromise risk).
e) Once this analysis has been undertaken, the relevant stakeholders must, in consultation with the Risk Management function, develop mechanisms to mitigate the identified risks and formally note them for the attention of the governing body for action.

7.2.4. Review of internal resources and policies for compliance with POPIA

Parallel to the POPIA Gap analysis and the analysis of what and how Personal Information is processed, the Project Manager must facilitate the alignment of internal processes and procedures with the respective measures noted and recommended to address the identified gaps. These must include but not be limited to;

7.2.4.1. Review of Bayport Policies and Procedures

Bayport shall on a continuous basis (and at least annually) review existing relevant policies to ensure that they are reasonable, appropriate and enforceable. All relevant policies must thus be reviewed by policy owners and must be approved by the Legal and Compliance Department (through the Project Manager) to ensure that they meet the aforementioned standards. This is inclusive of the review of the PAIA manual and privacy notices to ensure alignment with the POPIA Privacy Policy.

7.2.4.2. Website and associated resources;

Bayport shall also review the Bayport digital resources (such as the Bayport website, Bayport mobile application, etc.) to ensure that the data processing practices are aligned to the POPIA Provisions. All relevant resources must (in consultation with the Project Manager) be reviewed by resource managers and all changes and amendments must be approved by the Legal and Compliance Department (through the Project Manager) to ensure that they meet the required standards. It is recommended that the respective resource managers;

a) Develop a checklist of what to review
b) Agree upon the rating scheme to be used
c) Use the opportunity, where appropriate, to implement “best practice” such as Cookie notifications, etc.
d) Develop and implement a remediation plan.

7.2.5. POPIA Compliance Management processes

The Information Officer, as the party responsible for ensuring Bayport’s compliance with POPIA, must develop and implement a POPIA Compliance Management process and it is recommended that such process include;

a) The development of a Personal Information lifecycle including acquisition, processing, retention, and destruction practices.
b) The development of reasonable and appropriate measures to ensure ongoing compliance including but not limited to self-assessments, health-checks and formal audits.
c) The development of a dashboard for POPIA compliance

7.2.6. Employee Training and Awareness

The Information Officer must also ensure that all Bayport employees are aware of their responsibilities towards the protection of their personal information and that of Customers, Partners, Contracted Service Providers, Contractors and Directors. As such, training and awareness programme must be developed and implemented and must include;

a) Training requirements as per POPIA
b) Bayport's ongoing commitment to Training and Awareness
c) Special needs training such as the IO/DIO roles.

8. Review and Update

This policy must be reviewed by the document owner through the relevant governing committees, annually or whenever there are significant changes that might have an impact on this policy.