PROTECTION OF PERSONAL INFORMATION POLICY

A MANUAL PREPARED IN ACCORDANCE WITH THE

PROTECTION OF PERSONAL INFORMATION ACT, NO 4 OF 2003

THE PALLIDUS GROUP

2025/2026

DEFINITIONS

"**Consent**"	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
"**Data Subject**"	means the person to whom personal information relates;
"**Information Officer**"	means, in relation to a private body, the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act ("**POPI**")
"**Person**"	means a natural person or a juristic person;
"**Personal Information**"	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

(a) 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;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) 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;

(g) the views or opinions of another individual about the person; and

(h) 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;

"**Processing**"	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –
	(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
	(b) dissemination by means of transmission, distribution or making available in any other form; or
	(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;
"**Regulator**"	means the Information Regulator established in terms of section 39;
"**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;

"**Special personal information**"	means personal information as referred to in section 26 of POPI. In this regard section 26 states that: A responsible party may, subject to section 27, **not** process personal information concerning –

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such information relates to -

i. the alleged commission by a data subject of any offence; or

ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.;

1. INTRODUCTION

1.1. This is the Protection of Personal Information Policy ("**the Policy**") in respect of Pallidus Group Holdings (Pty) Ltd, Registration Number: 2020/188982/07 ("**Pallidus**").

1.2. This Policy applies to all persons and entities who, by virtue of their relationship with Pallidus, have access to Personal Information. This includes, but is not limited to, employees, contractors, consultants, service providers, board members, and other third parties acting on behalf of or in partnership with Pallidus. Adherence to this Policy is compulsory and non-compliance may lead to disciplinary action, legal liability, or termination of the business relationship.

1.3. The Policy outlines the rights of Data Subjects—being natural or juristic persons whose Personal Information is collected, stored, or processed by Pallidus—and establishes the procedures and principles to ensure lawful and responsible information management.

1.4. This Policy must be read in conjunction with Pallidus' PAIA Manual, IT & Cyber Risk Policy and Business Continuity Policy ("**Information Governance Policies**"). The Information Governance Policies form the foundation of Pallidus' approach to data protection, regulatory compliance and operational resilience.

2. PURPOSE

2.1 This Policy is intended to ensure that Pallidus:

2.1.1 Complies with all applicable data protection laws, including POPI;

2.1.2 Protects the privacy and confidentiality of Data Subjects' Personal Information;

2.1.3 Provides clear guidance on how Personal Information is collected, used, stored, disclosed, and deleted; and

2.1.4 Outlines the purposes for which such information is processed.

3. POLICY

3.1 Pallidus is committed to protecting the privacy of Data Subjects and to ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

3.2 We subscribe to the POPI principles and will:

3.2.1 Obtain and process information fairly;

3.2.2 Keep information only for one or more specified, explicit, and lawful purposes;

3.2.3 Use and disclose information only in ways compatible with these purposes;

3.2.4 Keep information safe and secure;

3.2.5 Keep information accurate, complete, and up to date;

3.2.6 Ensure that information is adequate, relevant, and not excessive;

3.2.7 Retain information for no longer than is necessary for the purpose or purposes; and

3.2.8 Provide a copy of personal data kept to the Data Subject on request.

4. PROCEDURES

4.1 Personal Information Collected

4.1.1 Pallidus collects and processes Personal Information in the course of conducting its operations. Pallidus will generally collect some of the following personal information from our Data Subjects:

4.1.1.1 Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, age, physical or mental health, well-being, disability, language, and birth;

4.1.1.2 Information relating to the education, medical, financial, criminal or employment history;

4.1.1.3 Identifying number, name, symbol, e-mail address, physical address, telephone number, location information;

4.1.1.4 Biometric information (employees);

4.1.1.5 Correspondence sent/received that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; and

4.1.1.6 The views or opinions of another individual about our Data Subject.

4.1.2 Pallidus enters into appropriate agreements with suppliers and service providers to ensure mutual compliance with personal information protection standards.

4.1.3 In addition to the information provided by our Data Subjects, we may also supplement this data with information received from trusted third-party providers. This allows us to enhance the accuracy, consistency, and relevance of the information we maintain, ultimately ensuring a more tailored and personalized experience for our clients when interacting with us.

4.2 How Personal Information is Used

4.2.1 Personal Information will only be used for the specific purpose for which it was collected and agreed upon. This may include:

4.2.1.1 Providing a product / service to a Data Subject;

4.2.1.2 As part of employee on-boarding or any other internal human resources function;

4.2.1.3 Conducting credit reference searches or verification;

4.2.1.4 Confirming, verifying, and updating contact details;

4.2.1.5 For the detection and prevention of fraud, crime, money laundering or other malpractice;

4.2.1.6 For audit and record keeping purposes;

4.2.1.7 In connection with legal proceedings;

4.2.1.8 Providing our services to a Data Subject to carry out the services requested and to maintain and constantly improve the relationship;

4.2.1.9 Providing communications in respect of Pallidus and regulatory matters that may affect Data Subjects;

4.2.1.10 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law;

4.2.1.11 To carry out the transaction(s) requested; and or

4.2.1.12 Conducting market or customer satisfaction research.

4.2.2 In terms of the provisions of POPI, Pallidus may only process personal information if one or more of the following conditions are met:

4.2.2.1 Consent – Processing is lawful if the Data Subject has provided explicit, voluntary, and informed consent. Consent is only required where the personal information is being used for a purpose other than the original intent/purpose for which it was provided.

4.2.2.2 Necessity of processing – The processing of Personal Information is necessary for the specific purpose at hand, such as fulfilling contractual obligations, providing requested services, or complying with regulatory requirements.

4.2.2.3 Legal obligation – Processing is lawful if it is necessary to comply with an obligation imposed by law, regulation, or legal framework that Pallidus is bound to follow.

4.2.2.4 Legitimate interests of the data subject – Processing is lawful if it is necessary to protect the legitimate interests of the Data Subject, provided these interests do not override the rights and freedoms of the Data Subject.

4.2.2.5 Legitimate interests of Pallidus or a third party – Processing is lawful if it is necessary for the pursuit of legitimate interests of Pallidus or a third party to whom the personal

information is supplied. However, Pallidus must ensure that such processing does not infringe upon the rights or freedoms of the Data Subject.

4.3 Disclosure of Personal Information

4.3.1 Pallidus will only disclose a Data Subject's Personal Information for purposes other than those for which it was originally collected in limited circumstances, including where:

4.3.1.1 we are legally required to do so in terms of applicable law, regulation, or court order;

4.3.1.2 such disclosure is necessary to establish, exercise or defend our legal rights; or

4.3.1.3 we are otherwise authorised to do so in accordance with the applicable data protection law.

4.3.2 We have confidentiality and data protection agreements in place with all relevant third parties to ensure that Personal Information is handled in accordance with the requirements of this Policy and applicable legislation.

4.3.3 Furthermore, we may share a client's Personal Information with, and obtain additional information from, authorised third parties, where necessary, to enhance service delivery, fulfil our obligations, and ensure a consistent and personalised client experience, as previously outlined.

4.4 Safeguarding Personal Information

4.4.1 We are committed to ensuring the security, integrity, and confidentiality of the Personal Information in our possession, as required by POPI. We implement and maintain appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of Personal Information, and to prevent unlawful access to or processing of such information. These safeguards are reviewed and updated on an ongoing basis in line with technological and regulatory developments.

4.4.2 Where we engage third-party service providers to process Personal Information on our behalf, we ensure that appropriate contractual and security obligations are in place to ensure compliance with POPI and to uphold the same standard of protection that we apply ourselves.

4.4.3 In some instances, we may transfer Personal Information to third parties or systems located in other countries. In doing so, we will ensure that such transfers comply with the conditions

for lawful cross-border data transfers under POPI, and that the recipient is subject to a law, binding agreement or corporate rules that provide an adequate level of protection for the processing of Personal Information.

4.5 Access and correction of Personal Information

4.5.1 Data Subjects have the right to request access to the Personal Information we hold about them. They may also request the correction, updating, or deletion of their Personal Information, provided that the request is based on reasonable grounds.

4.5.2 If a Data Subject objects to the processing of their Personal Information, and the objection is valid in terms of POPI, Pallidus may no longer process that information, unless permitted or required to do so by law or contract.

4.5.3 To safeguard the integrity and confidentiality of Personal Information, we will take all reasonable steps to verify the identity of the requesting Data Subject before providing access to, or making any changes to, their Personal Information. This process will be managed by Pallidus' designated Information Officer.

4.6 Data breaches

4.6.1 Even though Pallidus will take every precaution to prevent a data breach, it acknowledges that a breach may still occur despite these precautions.

4.6.2 A personal data breach is a breach of security that leads to one or more of the following:

4.6.2.1 **Confidentiality breach** – the accidental or unauthorised disclosure of, or access to, Personal Information;

4.6.2.2 **Availability breach** – the accidental or unauthorised loss of access to, or destruction of, Personal Information; and/or

4.6.2.3 **Integrity breach** – the accidental or unauthorised alteration of Personal Information.

4.7 Notification to the Information Regulator ("IR")

4.7.1 The Information Regulator must be notified of a personal data breach where it is likely to result in a risk to the rights and freedoms of Data Subjects. Such risks may include, for example:

4.7.1.1 loss of control over their data;

4.7.1.2 limitation of their rights;

4.7.1.3 discrimination;
4.7.1.4 identity theft;
4.7.1.5 fraud;
4.7.1.6 damage to reputation;
4.7.1.7 financial loss;
4.7.1.8 unauthorised reversal of pseudonymisation;
4.7.1.9 loss of confidentiality; and
4.7.1.10 any other significant economic or social disadvantage.

4.7.2 Where a security compromise is identified as reportable in terms of POPIA, Pallidus must notify the Information Regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach. If it is not possible to notify the Information Regulator within 72 hours, Pallidus must provide a written explanation for the delay as part of the notification.

4.7.3 The notification must at least include:
4.7.3.1 a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records;
4.7.3.2 the name and contact details of the Information Officer;
4.7.3.3 a description of the likely consequences of the breach; and
4.7.3.4 a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

4.8 Communication to affected Data Subjects

4.8.1 Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, Pallidus also needs to communicate the breach to the affected data subjects without undue delay, i.e., as soon as possible.
4.8.2 Reporting to Data Subjects may however be delayed if reporting may lead to an increased risk to the Data Subject.

4.8.3 In clear and plain language, Pallidus must provide affected Data Subjects with:
4.8.3.1 a description of the nature of the breach;
4.8.3.2 the name and contact details of Pallidus' Information Officer and CEO;
4.8.3.3 a description of the likely consequences of the breach;

4.8.3.4 a description of the measures taken, or to be taken, by Pallidus to address the breach and mitigate its possible adverse effects;

4.8.3.5 practical advice on how to limit the damage, e.g., resetting their passwords; and

4.8.3.6 Data subjects will be contacted individually, by e-mail, unless that would involve Pallidus in disproportionate effort such as where contact details have been lost as a result of the breach or were not known in the first place, in which case we will use a public communication, such as a notification on our website.

4.8.4 However, Pallidus is not required to report the breach to Data Subjects if:

4.8.4.1 appropriate technical and organisational protection measures have been implemented, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or

4.8.4.2 subsequent measures were taken to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise.

4.8.5 Communication to Data Subjects with regards to Data Breaches may under no circumstances be communicated or published without prior approval of Pallidus' Information Officer.

4.9 Data breach register

4.9.1 Pallidus will maintain a comprehensive and up-to-date Data Breach Register that records all actual or suspected personal information breaches, regardless of whether such breaches are notifiable to the Information Regulator in terms of POPI. The register will include, at a minimum, the following information for each incident:

4.9.1.1 The date and time the breach occurred (or was discovered);

4.9.1.2 A description of the nature of the breach;

4.9.1.3 The categories of personal information affected;

4.9.1.4 The number of data subjects potentially impacted;

4.9.1.5 The cause or suspected cause of the breach;

4.9.1.6 Actions taken to investigate, contain, and mitigate the breach;

4.9.1.7 Whether the Information Regulator and/or affected data subjects were notified;

4.9.1.8 The outcome of the internal investigation; and

4.9.1.9 Any corrective actions taken to prevent a recurrence.

4.10 Data breach reporting procedure

4.10.1 Any employee, contractor, or third party who becomes aware of, or suspects, a personal information breach must immediately report the incident to the Chief Operating Officer (COO) of Pallidus.

4.10.2 All available evidence and documentation relating to the breach—such as emails, access logs, screenshots, or system alerts—must be secured and retained to support a thorough investigation.

4.10.3 Pallidus takes the protection of personal information seriously. Employees are reminded that failure to report a known or suspected breach may constitute misconduct and could lead to disciplinary action in accordance with the organisation's internal policies and procedures.

4.11 Response plan

4.11.1 According to Pallidus' response plan the Deputy Information Officer will:

4.11.1.1 Make an urgent preliminary assessment of what data has been lost, why and how;

4.11.1.2 Take immediate steps to contain the breach and recover any lost data;

4.11.1.3 Undertake a full and detailed assessment of the breach;

4.11.1.4 Record the breach in Pallidus' data breach register;

4.11.1.5 Notify the Information Regulator where the breach is likely to result in a risk to the rights and freedoms of data subjects;

4.11.1.6 Notify affected Data Subjects where the breach is likely to result in a high risk to their rights and freedoms; and

4.11.1.7 Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

4.11.2 Please see Annexure "A" for more information.

4.12 Information Officer and Deputy Information Officer

4.12.1 POPI appoints the highest level of authority in an organisation as the Information Officer. The Information Officer has been tasked with ensuring compliance with data protection and privacy legislation and regulations.

4.12.2 The Information Officer has appointed a Deputy Information Officer to perform the required tasks.

4.12.3 The details of our Information Officer and Deputy Information Officer are as follows:

Information Officer

Name and Surname: Robyn van Heerden
Regulator Registration Number: TBC

Deputy Information Officer

Name and Surname: Caelin Coppinger
Regulator Registration Number: TBC

Our Information Officer and Deputy Information Officer are contactable at our Head Office:

Telephone Number: 012 880 2490
Physical Address: Die Groenhuis, 38 Garsfontein Road, Waterkloof, Pretoria,0145
Email Address: stephan@pallidus.co.za / compliance@pallidus.co.za
Website: www.pallidus.co.za

5. CONSEQUENCES OF NON-ADHERENCE

5.1 Pallidus will conduct regular compliance monitoring to ensure adherence to the requirements and principles set out in this Policy. Monitoring outcomes will be reported to the Information Officer for review and, where necessary, escalation.

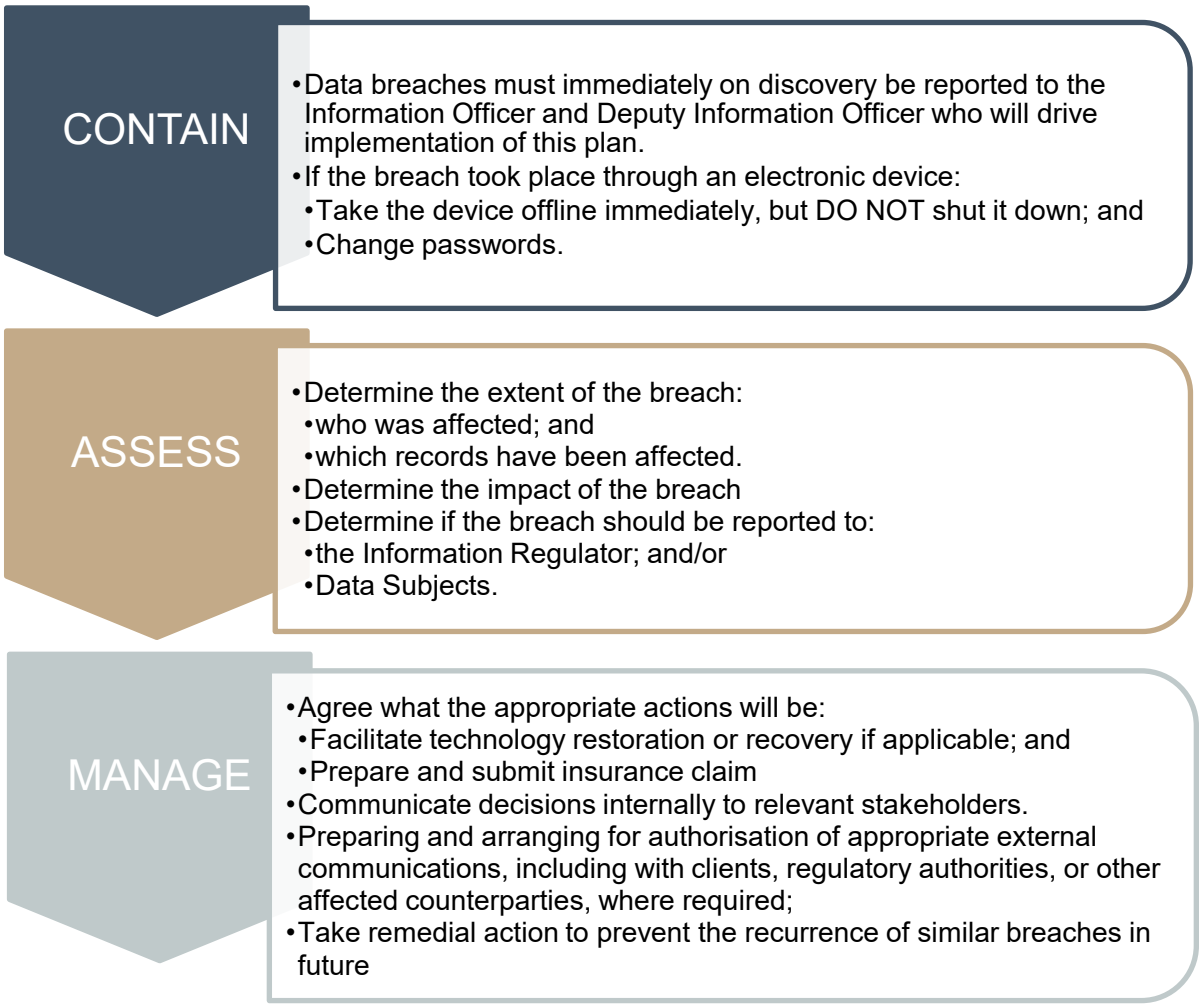
5.2 Any employee, contractor, or third party who fails to comply with this Policy may be subject to corrective or disciplinary action, which may include warnings, retraining, suspension, termination of employment or contract, or any other action deemed appropriate in accordance with Pallidus' internal disciplinary procedures and applicable legislation.

5.3 Non-compliance with this Policy may also expose Pallidus to legal, regulatory, and reputational risks, and will be treated with the appropriate level of seriousness.

6. TRAINING AND AWARENESS

Pallidus is committed to ensuring that all relevant staff understand their obligations under this Policy and POPI. To this end, appropriate training and awareness initiatives will be implemented on a regular basis. Training will cover key responsibilities, data handling procedures, breach reporting obligations, and the consequences of non-compliance. Records of all training completed will be retained for audit and compliance purposes.

Annexure A


CONTAIN
•Data breaches must immediately on discovery be reported to the Information Officer and Deputy Information Officer who will drive implementation of this plan.
•If the breach took place through an electronic device:
•Take the device offline immediately, but DO NOT shut it down; and
•Change passwords.
ASSESS
•Determine the extent of the breach:
•who was affected; and
•which records have been affected.
•Determine the impact of the breach
•Determine if the breach should be reported to:
•the Information Regulator; and/or
•Data Subjects.
MANAGE
•Agree what the appropriate actions will be:
•Facilitate technology restoration or recovery if applicable; and
•Prepare and submit insurance claim
•Communicate decisions internally to relevant stakeholders.
•Preparing and arranging for authorisation of appropriate external communications, including with clients, regulatory authorities, or other affected counterparties, where required;
•Take remedial action to prevent the recurrence of similar breaches in future