LUCID CARE (PTY) LTD

DATA BREACH POLICY

MARCH 2026 – VERSION 1

TABLE OF CONTENTS

Table of Contents

DATA BREACH POLICY

1. Purpose

1.1. This document is the Data Breach Policy ("DBR Policy") of Lucid Care Proprietary Limited ("the Company") which provides a plan as to the procedures if there is an actual or suspected Data Breach.

1.2. This Policy identifies and describes the roles and responsibilities of the Incident Response Team to report suspected thefts involving data, data breaches or exposures (including unauthorised access, use, or disclosure) to appropriate Data Subjects; and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

1.3. This DBR Policy is intended to enable the Company to promptly and comprehensively assess, contain, respond to and remediate Data Breach Incidents through:

1.3.1. mitigating the impact of a Data Breach Incident on the Company, its customers, clients, employees, Data Subjects and others;

1.3.2. ensuring all actions are documented when responding to a Data Breach Incident;

1.3.3. ensuring Data Breach Response Team members are appropriately engaged; and

1.3.4. implementing continual improvements to the DBR Policy.

1.4. The Company is subject to the following additional legislative, regulatory and Company specific policy obligations:

1.4.1. The Protection of Personal Information Act, 4 of 2013 ("POPI");

1.4.2. The Promotion of Access to Information Act, 2 of 2000 ("PAIA") ;

1.4.3. The Cybercrimes Act 19 of 2020;

1.4.4. Regulations published from time to time by the Information Regulator (South Africa); and

1.4.5. The Company's Policies.

2. Scope

2.1 This DBR Policy applies to the Company's business groups, divisions and subsidiaries, their employees, contractors, officers and directors.

2.2 This DBR Policy also applies to any third-party service provider and their personnel who access the Company's information technology systems, network, data, computer systems or networks connected to the Company's network.

2.3 The Data Breach Incident Response Coordinator is responsible for maintaining this DBR Policy.

2.4 Actions contrary to this DBR Policy (including violations of the DBR Policy) may result in disciplinary action.

3. Definitions

The terms defined in this clause 3 apply throughout this DBR Policy:

3.1. **Confidential Information ("CI") Data Breach:**

3.1.1 loss or theft of Confidential Information (for example, lost portable storage device containing confidential monthly sales information); or

3.1.2 unauthorised use, disclosure, acquisition of or access to, or other unauthorised processing of Confidential Information;

3.1.3 Any act that has or might reasonably be expected to compromise the confidentiality, integrity or availability of Confidential Information (for example, unauthorised access to human resource systems or unauthorised publishing of budget related information).

3.2. **Confidential Information:** information, which is not publicly available and which, if improperly disclosed or lost, may cause harm to the Company [or its customers, clients, employees, or other entities or individuals] but excludes Personal Information.

3.3. **Data Breach Incident Response Coordinator:** the nominated individual within the Company or the third-party service provider who is responsible for coordinating and responding to reports of Data Breach Incidents.

3.4. **Data Breach Incident:** types of data breach incidents including CI Data Breach, Personal Information Data Breach and Security Breach.

3.5. **Data Subject:** means the person to whom Personal Information relates.

3.6. **Impact Severity:** the severity of the impact of a Data Breach Incident is categorised as Impact Severity: Low, Impact Severity: Medium or Impact Severity: High with respect to factors such as:

3.6.1 whether the incident has arisen within the Company, or externally;

3.6.2 whether the incident is the result of a malicious attack or an accident;

3.6.3 whether Personal Information is involved, and if so, what type of Personal Information;

3.6.4 whether Confidential Information is involved, and if so, what type of Confidential Information;

3.6.5 how many Data Subjects are affected;

3.6.6 whether there is a risk to an individual's /Data Subject's safety or likelihood of harm to an individual;

3.6.7 whether there is a threat to the Company's systems;

3.6.8 whether there is a threat to the Company's ongoing business capacity;

3.6.9 whether there is a threat to the Company's financial interests;

3.6.10 to what extent there is potential for damage to Company's reputation; and

3.6.11 whether the incident is contained or ongoing.

3.7. **Impact Severity: Low:** the Data Breach Incident has a mix of the characteristics assessable under Impact Severity, and most of the following are true or anticipated to be true in the circumstances for the Data Breach Incident:

3.7.1. internal incident;

3.7.2. result of an accident;

3.7.3. no Personal Information involved;

3.7.4. Confidential Information involved;

3.7.5. limited Data Subjects affected;

3.7.6. no risk to an individual's/Data Subject's safety or risk of harm to an individual/ Data Subject;

3.7.7. no threat to Company's systems;

3.7.8. no threat to Company's ongoing business capacity;

3.7.9. no threat to Company's financial interests;

3.7.10. little to no potential for damage to Company's reputation; and

3.7.11. the incident is contained.

3.8. **Impact Severity: Medium:** the Data Breach Incident is neither Impact Severity: Low nor Impact Severity: High but has a mix of the characteristics assessable under Impact Severity.

3.9. **Impact Severity: High:** the Data Breach Incident has a mix of the characteristics assessable under High Impact Severity, and most of the following are true or anticipated to be true in the circumstances for the Data Breach Incident:

3.9.1. external incident;

3.9.2. malicious attack;

3.9.3. Personal Information is involved;

3.9.4. Confidential Information is involved;

3.9.5. multiple Data Subjects are affected;

3.9.6. likely risk to an individual's safety or likelihood of harm to an individual;

3.9.7. threat to Company's systems;

3.9.8. threat to Company's ongoing business capacity;

3.9.9. threat to Company's financial interests;

3.9.10. significant potential for damage to Company's reputation; and

3.9.11. the incident is ongoing.

3.10. **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:

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

3.10.2. Special Personal 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, the biometric information of the person, the personal opinions, views or preferences of the person, information relating to the education or the medical, financial, criminal or employment history of the person;

3.10.3. 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.

3.11. **Personal Information ("PI") Data Breach:**

3.11.1. loss or theft of Personal Information (for example, lost laptop or portable storage device containing Personal Information); or

3.11.2. unauthorised use, disclosure, acquisition of or access to, or other unauthorised processing of Personal Information (for example, unauthorised publication of Personal Information to an uncontrolled environment like a third party website).

3.12. **Post Incident Review Team:** the DBR Team, the Data Breach Incident Response Coordinator and any other key individuals who participated in the response to the Data Breach Incident.

3.13. **Security Breach:** unauthorised access to or use of, inability to access, loss or theft of, or malicious infection of the Company's IT systems, applications or devices, or connected third party systems (for example, unauthorised access to the network environment).

4. Data Breach Response Team

4.1. The data breach response team (DBR Team) for the Company can be found in **Annexure A**.

4.2. The Company authorises the DBR Team to take necessary actions to mitigate, contain and resolve Data Breach Incidents, in accordance with this DBR Plan, with the aims of:

4.2.1. avoiding loss of or damage to the Company's information technology systems, network, and data;

4.2.2. minimising economic, reputational, or other harms to the Company and its customers, clients, employees, and affiliates; and

4.2.3. managing notification to affected individuals, law enforcement, litigation and other risks.

4.3. The DBR Team is accountable for:

4.3.1. promptly addressing Data Breach Incidents according to this DBR Plan:

4.3.1.1. ensuring Data Breach Incidents are promptly detected and reported;

4.3.1.2. investigating and determining the nature and scope of the Data Breach Incident including procuring a root cause analysis;

4.3.1.3. containing the Data Breach Incident and managing recovery activities;

4.3.1.4. preserving evidence;

4.3.1.5. making notifications to the affected individual/Data Subjects and the Information Regulator, and responding to any litigation or enforcement action;

4.3.1.6. communicating internally within the Company as appropriate:

4.3.1.6.1. limiting the Company's internal communications regarding the details of the Data Breach Incident to a need-to-know basis;

4.3.1.6.2. notifying employees and other internal stakeholders of the Company as soon as the Data Breach Incident is contained and basic facts are known;

4.3.1.6.3. considering whether the Company's employees are also affected persons that must receive individual notification; and

4.3.1.6.4. issuing a policy statement to the Company's employees regarding external communication with media or third parties.

4.3.1.7. communicating externally as required to individuals /Data Subjects (including to business partners, clients and stakeholders / third parties) to limit damage to the Company's reputation and capacity for ongoing business;

4.3.1.8. performing post-incident reviews to improve the effectiveness of the DBR Plan, capture learnings and remedy any security or technology gaps (as applicable) to reduce the likelihood of a Data Breach Incident in the future.

4.3.2. advising and directing the Company within the scope of their expertise and knowledge of the Company's business;

4.3.3. reprioritising any other work responsibilities to give precedence to their roles in responding to the Data Breach Incident;

4.3.4. managing internal and external communications regarding Data Breach Incidents, including with the media on behalf of the Company; and

4.3.5. reporting their findings to the management of the Company and to applicable authorities, as appropriate.

4.4. The Leader of the DBR Team is responsible for all elements of managing the DBR Team and the Company's response to the Data Breach Incident.

4.5. The Administrator of the DBR Team is responsible for:

4.5.1. establishing a secure, physical space and distributing contact information such as password, log-in, dial-in details for the DBR Team to meet whenever required;

4.5.2. coordinating members of the DBR Team and the activities of their respective workstreams;

4.5.3. scheduling meetings of the DBR Team on request of the Leader of the DBR Team, and keeping minutes of those meetings; and

4.5.4. documenting the actions taken by DBR Team members at each stage of the response to the Data Breach Incident.

4.6. All members of the DBR Team are answerable to the Leader of the DBR Team for all matters relating to the Data Breach Incident.

4.7. The following external resources are to be made available to the DBR Team at the time of the Data Breach Incident, if required:

4.7.1. External public relations;

4.7.2. Forensic information technology services;

4.7.3. External legal counsel;

4.7.4. Supplementary printers/mailing house;

4.7.5. Supplementary call centre facilities;

4.7.6. Any other external experts.

5. Identifying a Data Breach Incident

5.1. Any types of Data Breach Incidents satisfying Impact Severity: Low, Impact Severity: Medium or Impact Severity: High as set out at **Clause 3** must be reported by any person to the Data Breach Incident Report Coordinator by:

5.1.1. email address: jim.beattie@lucidcx.com **;**

5.1.2. phone number: **082 410 3660**

5.2. An individual/Data Subjects should report any Data Breach Incident they discover or suspect immediately as required above and must not engage in their own investigation or other related activities unless authorised in writing by the DBR Team.

5.3. External sources who claim to have information regarding an actual or alleged Data Breach Incident should be directed to the Data Breach Incident Response Coordinator.

5.4. An individual/Data Subject who receives emails or other communications from external sources regarding a Data Breach Incident that may affect the Company or others shall immediately report those communications to the Data Breach Incident Response Coordinator and will not interact with the source unless authorised by the DBR Team.

5.5. A Data Breach Incident Report Template can be found in **Annexure B**.

6. Escalation

6.1. When a Data Breach Incident is reported to the Data Breach Incident Response Coordinator, the Data Breach Incident Response Coordinator will perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including:

6.1.1. affected systems and data;

6.1.2. potential risks and impact to the Company;

6.1.3. potential risks and impact to the Company's stakeholders / third-parties, clients, employees, or others;

6.1.4. whether the incident involves Personal Information, Confidential Information or other information;

6.1.5. the likelihood of harm to any of the individuals/Data Subjects affected by the Data Breach Incident based on the report to the Data Breach Incident Response Coordinator with consideration of harm such as:

6.1.5.1. identity theft;

6.1.5.2. significant financial loss by the individual/Data Subject;

6.1.5.3. threats to an individual/Data Subject's physical safety;

6.1.5.4. loss of business or employment opportunities;

6.1.5.5. humiliation, damage to reputation or relationships.

6.1.6. the type of Data Breach Incident (if known); and

6.1.7. the expected Impact Severity level of the Data Breach Incident (if known).

6.2. An Assessment of Severity of the Data Breach Incident can be found in **Annexure C**.

6.3. Based on the initial assessment, the Data Breach Incident Response Coordinator, or their delegate, will:

6.3.1. notify the DBR Team about the Data Breach;

6.3.2. the Data Breach Incident as reported;

6.3.3. the type of Data Breach Incident; and

6.3.4. the initial assessment of the Impact Severity level.

6.3.5. activate the DBR Team by scheduling the initial DBR Team meeting to occur urgently within the next:

6.3.5.1. 30 minutes for Impact Severity: High;

6.3.5.2. 60 minutes for Impact Severity: Medium; and

6.3.5.3. 120 minutes for Impact Severity: Low.

7. Activation of the DBR Team

7.1. Once activated by the Data Breach Incident Response Coordinator, the DBR Team will meet and work together to:

7.1.1. investigate the Data Breach Incident;

7.1.2. isolate the cause of the Data Breach Incident;

7.1.3. confirm or alter the type of Data Breach Incident;

7.1.4. confirm or alter the Impact Severity level of the Data Breach Incident;

7.1.5. analyse the impact of the Data Breach Incident and its likely effects on the Company and whomever is also impacted (including affiliates and individuals);

7.1.6. strategize a formulated response plan to contain, remediate, and recover from the Data Breach Incident;

7.1.7. collect information about the Data Breach Incident itself, including:

7.1.7.1. how the breach was discovered;

7.1.7.2. the nature of the breach (for example, whether systems were compromised or hardware lost);

7.1.7.3. the date and time of the breach;

7.1.7.4. the duration and location of the breach;

7.1.7.5. the method of system infiltration (if applicable);

7.1.7.6. the compromised systems, files or data;

7.1.7.7. whether Personal Information was accessed or is accessible; and

7.1.7.8. whether Confidential Information was accessed or is accessible.

7.1.8. collect details about the compromised data, including:

7.1.8.1. a list of affected Data Subjects;

7.1.8.2. the types of affected data;

7.1.8.3. the number of records affected; and

7.1.8.4. whether any of the data was encrypted.

7.1.9. identify which member of the DBR Team will be responsible for and oversee each workstream of the response plan as formulated, and report to the Leader of the DBR Team for that work stream;

7.1.10. notify the board of directors or any other appropriate senior executive of the Company of the Data Breach Incident and of the Impact Severity: High or Medium or Low;

7.1.11. enlist the services of external resources in **Clause 4.7** as appropriate;

7.1.12. prepare a media holding statement so the Company can make an announcement quickly if required.

7.1.13. designate a member of the DBR Team, or their delegate, to be the contact person for all media [and law enforcement] enquiries; and

7.1.14. schedule the next DBR Team meeting according to the Impact Severity level:

7.1.14.1. within two hours for an Impact Severity: High;

7.1.14.2. within six hours for an Impact Severity: Medium; or

7.1.14.3. at the same time the next day for an Impact Severity: Low.

7.2. The DBR Team will repeat the steps outlined in **Clause 7.1** as relevant to execute the response plan it formulates, and as required according to its investigation and analysis, to contain, remediate and recover from the Data Breach Incident, using appropriate internal and external resources.

7.3. The Administrator of the DBR Team will document:

7.3.1. a timeline of the Data Breach Incident including the DBR Team's meetings and actions;

7.3.2. the DBR Team's response plans;

7.3.3. minutes of the DBR Team's meetings; and

7.3.4. each of the activities commenced by the DBR Team under each of its workstreams.

7.4. The DBR Team will direct internal and external resources to capture and preserve evidence related to the Data Breach Incident.

7.5. The DBR Team will engage the Company's Board of Directors, or their delegate, to determine whether additional handling or preservation procedures are required, and to what extent the data breach response activities should be protected by legal professional privilege.

8. Communications

8.1. The DBR Team will be responsible for coordinating the content and timing of communications, and if necessary, with the external public relations agency:

8.1.1. internally within the Company as appropriate considering the characteristics and circumstances of the Data Breach Incident, providing resources to appropriately direct questions from stakeholders / third-parties, clients, media, Data Subjects or others;

8.1.2. to the Company's leadership on a regular basis, explaining the Data Breach Incident and its potential impact on the Company, its stakeholders / third-parties, clients, employees, Data Subjects and others as details become available;

8.1.3. to other related stakeholders including suppliers, affiliates and business partners as appropriate considering the characteristics and circumstances of the Data Breach Incident;

8.1.4. to the public including the media, [as appropriate OR as necessary and advised by the external public relations agency] using the Company's website, press releases or other means; and

8.1.5. to law enforcement as required, and in the event of any criminal activity or threats as the DBR Team considers appropriate in the circumstances.

8.2. Only the DBR Team may authorise the distribution of communications (including notifications at **Clause 10**) related to the Data Breach Incident.

8.3. The DBR Team will obtain the view and advice of the Company's internal or external legal counsel, for any communications (including notifications at **Clause 10**) related to the Data Breach Incident.

8.4. Specifically, the DBR Team will consider:

8.4.1. setting up a dedicated phone number / email address to field calls / emails and questions from affected individuals/Data Subjects;

8.4.2. preparing a script for telephone or email and establishing an escalation process for enquiries that the Company's usual reception personnel are unable to handle;

8.4.3. preparing frequently asked questions (FAQs) for responding to affected individuals' enquiries; and

8.4.4. posting information on the Company's website.

9. Legal Review

9.1. The DBR Team will engage with the Company's internal or external legal counsel to undertake the activities in **Clause 9.2** to **Clause 9.5** (inclusive) and report on each activity to the DBR Team.

9.2. Assess the risk of litigation or regulatory action against the Company resulting from the Data Breach Incident.

9.3. Determine the Company's liability and indemnification obligations or rights resulting from the Data Breach Incident, including whether:

9.3.1. any third parties have any such obligations to the Company; and

9.3.2. the Company has any such obligations to third parties.

9.4. If the Data Breach Incident involves a third party:

9.4.1. reach out to the third party as soon as possible.

9.4.2. foster a cooperative relationship with the third party to mitigate the damage that may arise from the Data Breach Incident;

9.4.3. if appropriate, designate an individual on the DBR Team to handle communications with the third party; and

9.4.4. identify whether the Data Breach Incident involves Personal Information that the Company holds for the third party, or the third party holds for the Company in which case:

9.4.4.1. the Information Regulator and affected Data Subjects must be notified; and

9.4.4.2. there is a contractual obligation on either party to make the notifications and otherwise which party will make those notifications.

9.5. Perform contract reviews of any contracts applicable to the Data Breach Incident and determine:

9.5.1. whether the Company has a claim or any liability for breach of a specific data protection or security obligation;

9.5.2. whether there may be a claim or any liability for breach of confidence or a failure to take reasonable skill and care;

9.5.3. whether the breach gives rise to a right for the Company or another party to claim damages, and if so, whether the value of the claim is limited;

9.5.4. how a claim for damages might be quantified, in particular whether there are liquidated damages, are costs resulting from the breach recoverable and other considerations such as service credits;

9.5.5. whether the Data Breach Incident gives rise to an express right to terminate a contract or alternatively whether the breach is sufficiently serious to give rise to the right to terminate the contract at common law;

9.5.6. whether the Data Breach Incident triggers any other aspects of a contract, such as audit rights or the implementation of business continuity and disaster recovery plans; and

9.5.7. whether there are any specific administrative matters that need to be adhered with to preserve rights, such as written notice provisions to particular individuals.

10. Notification

10.1. The DBR Team should take necessary actions to prioritise necessary notifications and avoid news of the Data Breach Incident reaching the media before notifying the Information Regulator and affected individuals.

10.2. the Company may be required to notify third parties, including affected individuals, as a matter of law, regulation or contractual commitment. As applicable in the circumstances of the Data Breach Incident, the DBR Team will prepare, coordinate, and ensure appropriate notifications. As applicable in the circumstances of the Data Breach Incident, the DBR Team will prepare, coordinate and ensure appropriate notifications are made to:

10.2.1. individuals;

10.2.2. the Company's insurer;

10.2.3. the Company's financial services provider;

10.2.4. professional associations; and

10.2.5. customers, clients and business partners according to current agreements.

10.3. If notification is necessary, the DBR Team will:

10.3.1. develop a notification plan;

10.3.2. prepare a notification timing schedule;

10.3.3. implement the notification plan in an expeditious and legally sufficient manner; and

10.3.4. keep a record of the type, date, recipient and contents of each notification.

10.4. For Data Breach Incidents involving Personal Information:

10.4.1. Where there are reasonable grounds to believe that Personal Information of a Data Subject has been accessed or acquired by an unauthorised person, the Company as the Responsible Party is obligated to notify:

10.4.1.1. The Information Regulator; and

10.4.1.2. The individual/Data Subject, unless the identity of the individual/Data Subject cannot be established.

10.4.2. The notification referred to in **Clause 10.4.1** is required to be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of Responsible Party's information system.

10.4.2.1. The Responsible Party may only delay notification of the individual/Data Subject if a public body responsible for prevention, detection or investigations of offences or the Information Regulator determines that the notification will impede a criminal investigation by the public body concerned.

10.4.3. The notification to the individual/Data Subject must be made in writing and communicated to the Data Subject in at least one of the following ways:

10.4.3.1. mailed to the individual/Data Subject's last known physical or postal address;

10.4.3.2. sent by email to the individual/Data Subject's last known email address;

10.4.3.3. placed in a prominent position on the website of the Responsible Party;

10.4.3.4. published in the news media; or

10.4.3.5. as may be directed by the Regulator.

10.4.4. The notification, an example of which can be found in **Annexure D**, must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including:

10.4.4.1. a description of the possible consequences of the security compromise;

10.4.4.2. a description of the measures that the Responsible Party intends to take or has taken to address the security compromise;

10.4.4.3. a recommendation with regard to the measures to be taken by the individual/Data Subject to mitigate the possible adverse effects of the security compromise; and

10.4.4.4. if known to the Responsible Party, the identity of the unauthorised person who may have accessed or acquired the Personal Information.

10.4.5. The Company should:

10.4.5.1. identify the jurisdictions where any affected persons may reside to assess whether any other province (or foreign country) breach notification laws may be triggered (for example, the General Data Protection Regulation in the European Union);

10.4.5.2. identify whether the type of Personal Information compromised, for instance medical information, triggers additional statutory obligations;

10.4.5.3. prepare and maintain a list or database of individuals/Data Subjects to be notified that includes:

10.4.5.3.1. the Data Subject's name and address;

10.4.5.3.2. other contact and identifying information for the Data Subject;

10.4.5.3.3. the affected information; and

10.4.5.3.4. the notification status.

10.4.5.4. determine whether to offer remediation services to affected individuals, such as:

10.4.5.4.1. credit monitoring services;

10.4.5.4.2. identity theft insurance; and

10.4.5.4.3. referral to other organisations that support individuals affected by data breaches.

11. Disciplinary Action

11.1. The Human Resources member of the DBR Team with the internal or external legal counsel and the Leader of the DBR Team will determine whether the Company should take any employment action against any responsible employees as a result of the Data Breach Incident, with consideration as to:

11.1.1. Any corporate requirements of the Company or any statutory requirements that may affect the way that the disciplinary process is conducted;

11.1.2. The Company's misconduct policies and other relevant policies, such as its privacy policy, information technology and internet use policy and

security policy to determine the extent to which the employee has breached their contractual obligations; and

11.1.3. Whether the employee had received adequate training and guidance on data protection and security responsibilities and ought reasonably to have been aware of the employer's requirements and the consequences of breaching them.

12. Post Incident Review

12.1. At a time reasonably following **OR** within 7 (seven) business days of a Data Breach Incident, the DBR Team Leader will convene the Post Incident Review Team for a post-incident review meeting to critically assess the Data Breach Incident and the Company's response.

12.2. The Post Incident Review Team will review the Company's response to the Data Breach Incident to identify any gaps, oversights or opportunities for improvement, specifically assessing:

12.2.1. the reporting process;

12.2.2. the activation of the DBR Team;

12.2.3. the collaboration of the DBR Team;

12.2.4. the usefulness of the DBR Plan;

12.2.5. the notification process; and

12.2.6. the Company's response to the Data Breach Incident generally.

12.3. The Post Incident Review Team will also confirm the root cause of the Data Breach Incident and make recommendations for minimising the risk of the same or similar recurrence.

12.4. The activities and findings of the Post Incident Review Team must be documented and provided to the CEO or Managing Director or the Board of Directors within 7 (seven) business days of the post-incident review meeting.

12.5. The Data Breach Incident Response Coordinator will coordinate and implement any follow-up actions or recommendations identified by the Post Incident Review Team, including making any amendments to this DBR Plan.

12.6. The Data Breach Incident can only be closed and the DBR Team disbanded when deemed appropriate by the Board of Directors, or their delegate in consultation with the Data Breach Incident Response Coordinator and the Leader of the DBR Team. The DBR Team should continue to meet at intervals appropriate to the circumstances of the Data Breach Incident until the Data Breach Incident is closed.

13. DBR Plan Training and Testing

13.1. The Data Breach Incident Response Coordinator is responsible for and will:

13.1.1. Develop, maintain, and deliver training on the DBR Plan to the Company's staff regularly across each year OR annually.

13.1.2. Ensure the Company's staff and especially those with access to Company's systems, network or data:

13.1.2.1. are aware of the DBR Plan;

13.1.2.2. are able to identify when a Data Breach Incident has occurred;

13.1.2.3. understand their unfettered obligation to report a Data Breach Incident to the Data Breach Incident Response Coordinator; and

13.1.2.4. understand how to report the Data Breach Incident to the Data Breach Incident Response Coordinator.

1.4.6. Educate members of the DBR Team on their roles and obligations when participating as a member of the DBR Team and responding to a Data Breach Incident.

1.4.7. Test the DBR Plan with the members of the DBR Team (including their designated alternates) against a set of different mock circumstances at least twice per year and capture any learnings in a revised DBR Plan as set out in **Clause 14**.

14. DBR Plan Amendments

14.1. The Company will review the DBR Plan at least annually and whenever there is a material change in the Company's business practices that may reasonably affect its Data Breach Incident response.

14.2. The Data Breach Incident Response Coordinator will update the DBR Plan as appropriate following post-incident reviews and testing exercises.

14.3. The Data Breach Incident Response Coordinator and the internal/external or their delegates, must approve changes to the DBR Plan in writing.

14.4. The Data Breach Incident Response Coordinator is responsible for the DBR Plan and will promptly update staff and management of the Company regarding any changes to the DBR Plan.

15. Effective Date

15.1. This DBR Plan is effective as of **6 March 2026**.

ANNEXURE A – DBR TEAM

Leader / Administrator of the DBR Team / Privacy / Compliance
Name: **James Henry Beattie**
Position: **Chief Executive Officer**
Contact phone number: **082 410 3660**
Contact email address: Jim.beattie@lucidcx.com
Deputy Leader
Name: **Tumelo Tladi**
Position: **Content and Customer Engagement Specialist**
Contact phone number: **072 418 8245**
Contact email address: tumelotladi@lucidcx.com
Legal Support
Name: **Goolam Norris**
Position: **Legal Advisor**
Contact phone number: **082 924 4127**
Contact email address: goolam@kvnlaw.co.za

ANNEXURE B - DATA BREACH INCIDENT REPORT

Data Breach Incident Report	
Date & time incident was discovered:	
Date(s) of incident:	
Place of incident:	
Department affected by the Data Breach Incident:	
Name of the person reporting the incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of the incident or details of the information lost:	
Incident scope - The department's determination of how widespread is the incident. Particularly relevant for the Company's Service Providers where one incident may affect multiple persons:	
Impact on the business:	

Incident type:	
Indicators of compromise (URL's, IP addresses, Email headers, Email addresses, Email subjects, Email body, Web Domains, File hashes, File types/files & Information Classification, Physical indicators, Other indicators of relevance):	
The number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If so, please provide details:	
Brief description of any action taken at the time of discovery:	
SAPS report and case number:	
For use by the Person reporting the incident:	
Received by:	
On (date):	
Forward for action to:	
On (date):	

ANNEXURE C – ASSESSMENT OF SEVERITY OF DATA BREACH INCIDENT

Assessment of Severity	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of the information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems/ the Cloud?	
Is the information unique? Will its loss have adverse operational, research, financial or legal liability or reputational consequences for the Company or third parties?	
How many Data Subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories: **Impact Severity: Low:**	

• internal incident; • result of an accident; • no Personal Information involved; • Confidential Information involved; • limited Data Subjects affected; • no risk to an individual's/Data Subject's safety or risk of harm to an individual/ Data Subject; • no threat to Company's systems; • no threat to Company's ongoing business capacity; • no threat to Company's financial interests; • little to no potential for damage to Company's reputation; and • the incident is contained. **Impact Severity: Medium:** The Data Breach Incident is neither Impact Severity: Low or Impact Severity: High but has a mix of the characteristics assessable under Impact Severity. **Impact Severity: High:** • external incident; • malicious attack; • Personal Information is involved; • Confidential Information is involved; • multiple people / Data Subjects are affected; • likely risk to an individual's safety or likelihood of harm to an individual; • threat to Company's systems; • threat to Company's ongoing business capacity; • threat to Company's financial interests;	

• significant potential for damage to Company's reputation; and • the incident is ongoing.	

ANNEXURE D - DRAFT NOTIFICATION OF SECURITY COMPROMISES TO DATA SUBJECTS

We regret to inform you that _____ **OR** we suffered a data breach that caused certain Personal Information as defined under the Protection of Personal Information Act, no. 4 of 2013, to be exposed.

Immediately on becoming aware of the data breach, we acted in accordance with our Data Breach Response Policy. The attendances that we have undertaken includes having our Data Response Team and security experts contain, manage and investigate the data breach.

All necessary safeguards and precautionary measures were adequately in place, and we can only assume that the penetration of our network/infrastructure was executed with skill and careful planning. There appears to be no known motive for the data breach, but we believe that we are dealing with sophisticated criminals.

As a precautionary measure our systems have been taken offline and you can interact with us through the following means:

1.
2.
3.

The actual nature and extent of the data breach is under investigation, and we cannot ascertain at this stage what Personal Information or other Confidential Information has been exposed.

Accordingly, we urge you to remain vigilant about your Personal Information appearing or being utilised in circumstances that you did not consent to or are aware of. In order to assist with our investigation, you are urged to report any suspicious activity regarding the processing of your Personal Information to us immediately.

The protection and preservation of your personal data and our systems is of paramount important to us and you can rest assured that we are doing all things necessary to resolve this unfortunate situation.

We will keep you posted on any new developments that arise.

We apologise in advance for any inconvenience or disruption that may have been caused by this unfortunate situation.

Please call **JAMES HENRY BEATTIE** at **082 410 3660 or** jim.beattie@lucidcx.com for updates.