Ndalamo Resources (Pty) Ltd
Living Into The Future

PROTECTION OF PERSONAL INFORMATION POLICY

DOCUMENT TYPE	**DATA BREACH AND INCIDENT RESPONSE POLICY**	
DOCUMENT NO	**CORP AFF DBIR: 18**	
REVISION / VERSION	**01**	
ISSUE DATE	**21 June 2024**	
APPROVAL	**CORPORATE AFFAIRS DIRECTOR**	**Minah Moabi**
	Signature	
	Date	21 JUNE 2024
	FINANCIAL DIRECTOR	**Mpho Nkhumeleni**
	Signature	
	Date	21 JUNE 2024
	CHIEF EXECUTIVE OFFICER	**Shammy Luvhengo**
	Signature	
	Date	21 JUNE 2024

Revision History

Revision Detail	Revision No.	Revision Date	Revision Approval (Name & Designation)	Signature
Version 1	Rev 01	01-06-2024	DIRECTOR: Minah Moabi	

TABLE OF CONTENTS

1. INTRODUCTION

1.1. This policy applies to all employees of Ndalamo Resources (Pty) Ltd. Ndalamo will be referred to as **"the Company"** throughout this document.

1.2. This policy serves principally as a guideline and may be departed from where circumstances warrant such departure.

1.3. The Company in its sole discretion may revise this policy. The details of any such revision will be disseminated and communicated to all employees.

1.4. The policy shall remain in force until such time as it is amended or replaced by another policy or procedure.

2. PURPOSE

2.1. This document applies to the employees, staff, workers and/or other individuals working or undertaking a role under or on behalf of the Company. The Company is defined as a responsible party in respect of all personal information it processes as per the Protection of Personal Information Act 4 of 2013 ("POPIA"). When the terms 'we', 'us' or 'our' are used it should be read as referring to the Company, unless otherwise specified.

2.2. When notifying the Information Regulator ("Regulator") of a personal data/information breach, this must be done "as soon as reasonably possible" where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. The responsible party must notify the Regulator and subject to subsection (4), the data subject, unless the identity of such data subject cannot be established.

2.3. Organisations, such as the Company, who act as responsible parties are encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach and to assess the risk it poses to individuals. Records of any data/personal

information breaches must be maintained, regardless of whether or not required to notify that the breach has taken place.

2.4. All staff have a responsibility for the information that they generate, manage, transmit and use are in line with POPIA. However, it is also their contractual duty to secure personal and confidential data/information at all times. Any person who knows or suspects that a breach of data/information security has occurred should report the breach immediately.

2.5. It is vital that the Company and all its staff take prompt action in the event of any actual, potential, or suspected breaches of data/personal information security or confidentiality to avoid the risk of harm to stakeholders or employees, damage to operational business and severe financial, legal and reputational costs to the Company.

2.6. The purpose of this policy and guide is to provide a distinctive framework for the reporting and managing of any data/personal information breaches affecting confidential, personal, or special category data/information (defined below) held by the Company. This policy and guide are a supplement to the Company's Privacy Policy, which iterates the Company's commitment to protecting the privacy rights of data subjects in accordance with POPIA.

2.7. Accordingly, all staff members of the Company have an important role to play when following the data/personal information security breach procedure, enabling the Company to comply with POPIA and avoid hefty fines.

3. PERSONAL DATA / INFORMATION BREACH

3.1. A data/personal information breach is '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data/information transmitted, stored or otherwise processed*'. One of the consequences of a personal data/information breach would be the Company being unable to ensure compliance with the confidentiality and integrity principle as outlined in POPIA. Breaches can be categorised based on the following information security principles;

3.1.1. Confidentiality breach – where there is an unauthorised or an accidental disclosure of, or access to, personal data/information.

3.1.2. Integrity breach – where there is an unauthorised or an accidental alteration of personal data/information.

3.1.3. Availability breach – where there is an accidental or an unauthorised loss of access to or, destruction of, personal data/information.

3.1.4. Loss or destruction breach – where personal data/information is lost or stolen.

3.2. It should be noted that, depending on the circumstances, a breach can concern confidentiality, availability and integrity of personal data/information at the same time, as well as any combination of these. Personal data/information security breaches which would fall into the above categories would include:

3.2.1. Disclosing confidential data/information to unauthorised individuals;

3.2.2. Loss or theft of paper records or portable devices containing personal or special category personal data/information e.g. laptops, PCs, tablets, mobile phones, USB, disks, etc.;

3.2.3. Inappropriate access controls on electronic folders/files/drives which allows unauthorised access/use of personal data/information;

3.2.4. Suspected breach of the Company's Information Security and Acceptable Use of Information policies;

3.2.5. Attempts to gain unauthorised access to computer systems e.g. phishing and/or hacking;

3.2.6. Records altered or deleted without appropriate consent/authorisation from the data/information subject;

3.2.7. Viruses or other attacks on IT equipment, systems or networks;

3.2.8. Breaches of physical security e.g. breaking into secure rooms or filing cabinets where confidential personal data/information is stored;

3.2.9. Confidential personal data/information left unlocked in accessible areas;

3.2.10. Unsecure disposal of confidential paper waste;

3.2.11. Leaving laptops/desktops unattended when logged on to a user account without locking the screen.

4. DATA/INFORMATION THIS POLICY APPLIES TO

4.1. All personal data/information created or received by the Company in any format (including paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely;

4.2. Personal data/information held on all the Company's IT systems managed centrally, and locally by individual departments/groups; and

4.3. Any other IT systems on which Company data/information is held or processed.

5. RESPONSIBLE PARTIES FOR MANAGING DATA/INFORMATION SECURITY BREACHES

5.1. Personal data/information security breaches are managed by the Company's Information Officer (IO) Vukani Thole.

5.2. In emergency data security breach situations, the Company will manage the incident under the direction of the IO.

6. PROCEDURES FOR REPORTING DATA/INFORMATION SECURITY BREACHES

6.1. In the event of a breach of data/information security occurring within the Company, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence.

6.2. If a personal data/information breach or potential or suspected personal data/information breach has been reported to and/or otherwise become aware of a personal data/information breach, please report this immediately to the IO or Director of Corporate Affairs and Subsidiaries Minah Moabi. The attached Data Security Breach Report form should also be completed and e-mailed to the IO as soon as possible after the initial reporting.

6.3. This report should record all relevant details of the incident and should be communicated to all relevant staff on a strictly confidential basis to ensure that a prompt and appropriate action is taken to resolve the breach incident.

6.3.1. The IO must then notify interested parties and stakeholders of the breach event.

6.3.2. In terms of POPIA "*as soon as reasonably possible*" to the IR where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person. The responsible party must notify the Regulator and subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

6.3.3. If the IO decides that the breach does not require reporting to the IR it should still be documented as a breach with an explanation justifying why it did not need to be reported to the IR.

7. PROCEDURE FOR MANAGING PERSONAL DATA/INFORMATION SECURITY BREACHES

When managing a personal data/information breach these five steps should be followed:

7.1. Identification and Initial Assessment

7.1.1. As soon as a personal data/information breach has occurred it must be reported immediately to your Head of Department and the IO. The IO will then liaise with Minah Moabi. The individual reporting the breach should also complete the attached Data Security Breach Report Form and e-mail it to the IO without delay. The report form will assist the IO in conducting the initial assessment of the breach in order to establish:

7.1.1.1. If a personal data/information security breach has in fact taken place;

7.1.1.2. If a personal data/information security breach has occurred, what data/information has been involved/affected;

7.1.1.3. The cause of the breach;

7.1.1.4. The extent of the breach and how many individuals have been affected;

7.1.1.5. The level of harm/risk to the individuals affected by the breach;

7.1.1.6. How the breach can be contained.

7.1.2. After the initial assessment of the breach the IO will, in consultation with Minah Moabi, liaise with the appropriate head of department to carry out a full investigation of the breach event. Should the breach be significant, the IO will also consider whether or not to establish a Breach Management Team made up of the appropriate Company staff and/or third parties e.g., insurers or lawyers to assist with the investigation. All records relating to the investigation will be retained by the IO.

7.1.3. The IO will use the undernoted table to determine the severity of the incident, and this will be recorded on part 2 of the Data/information Security Breach Report Form. Depending on the level of the breach, the IO will decide whether the incident can

be managed/controlled at a local level or if it must be escalated to the Company's Executive team. If the IO deems the severity of the breach to be level 3 or above, then the Executive will be actively involved in the management of the event.

7.2. Containment and Recovery

7.2.1. Once established that a data/information breach has occurred the Company must take immediate and appropriate action to limit the breach. Accordingly, the IO with assistance from Minah Moabi will:

7.2.1.1. Establish who within the Company needs to be made aware of the breach and advise them what needs to be done to contain the situation;

7.2.1.2. Establish if anything can be done to recover any lost data/information and limit the damage of the breach e.g. physical recovery of the records, restoration of the data/information via back-up tapes;

7.2.1.3. Establish if it is appropriate to notify affected data subjects immediately i.e. where the risk/harm to the data subjects has been deemed as serious.

7.2.2. If appropriate, inform the Police in cases which involve data/information theft or other criminal activity relating to personal data/information.

7.3. Risk Assessment

7.3.1. Although POPIA introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances. Upon becoming aware of a breach, it is vitally important that the Company carries out a risk assessment of the breach and seeks to contain the incident.

7.3.2. In assessing the risk arising from a personal data/information breach, the IO along with all relevant members of the Company, are required to consider the potential adverse impact on data subjects i.e. what is the likelihood of actual harm to the affected data subjects is and how serious or substantial is the impact likely to be.

The information completed at Section 1 of the Data / Information Security Breach Report Form will assist with this part of the risk assessment.

7.3.3. The IO, along with the relevant the Company head of department of the area where the breach occurred, will review the breach report in order to assess the risks and consequences of the breach for both the data subjects involved and for the Company.

7.3.4. Risks for Data subjects:

7.3.4.1. Risk for the affected data subjects i.e. adverse consequences of the breach and how substantial/serious it is;

7.3.4.2. Likelihood of recurrence.

7.3.5. Risks for the Company:

7.3.5.1. Strategic and operational;

7.3.5.2. Compliance and legal;

7.3.5.3. Financial;

7.3.5.4. Business continuity;

7.3.5.5. Reputational damage.

7.3.6. Consideration must also be given to the following:

7.3.6.1. What type of personal data/information has been involved in the breach? I.e. Is it a special category of personal data/information;

7.3.6.2. Was the data/information protected in any way? E.g. Encryption which would make it less accessible;

7.3.6.3. What has actually happened to the data/information in question?

7.3.6.4. If it has been stolen, could the type of data/information be used for other purposes which would be of significant harm to the data subjects involved;

7.3.6.5. How many data subjects have been affected by the personal data/information breach? The assumption should not necessarily be that the risks are greater where large amounts of data/information have been lost. However, this is a vital factor to be considered and scrutinised;

7.3.6.6. Whose personal data/information is the subject of the breach? I.e. is it the Company staff, stakeholders, customers? This will, to some extent, determine the level of risk posed by the breach and will also direct the actions in mitigating the risks;

7.3.6.7. What harm could come to the data subjects affected by the breach? Are there potential risks to their physical safety, financial security or reputation or a combination of these factors?

7.3.7. Personal data/information breaches that are likely to result in high risk to the rights and freedoms of individuals would be circumstances where the breach may lead to physical, material or non-material damage for the individuals whose data/information have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data/information that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data/information, data/information concerning health or data/information concerning sex life, or criminal convictions and offences or related to security measures, such damage should be considered likely to occur.

7.3.8. The IO should determine, where appropriate, what remedial action should be taken on the basis of the breach report to mitigate the impact of the breach and also to ensure that the breach does not recur.

7.3.9. The IO will prepare an incident report which will set out, where applicable, the following:

7.3.9.1. A summary of the security breach;

7.3.9.2. The individuals involved in the security breach (such as employees, contractors, external clients);

7.3.9.3. Details of the information, the Company's IT systems, equipment or devices involved in the security breach and any information lost or compromised as a result of the incident;

7.3.9.4. How the breach occurred;

7.3.9.5. Actions taken to resolve the breach;

7.3.9.6. Impact of the security breach;

7.3.9.7. Unrealised, potential consequences of the security breach;

7.3.9.8. Possible courses of action to prevent a repetition of the security breach;

7.3.9.9. Side effects, if any, of those courses of action; and

7.3.9.10. Recommendations for future actions and improvements in data/information protection as relevant to the breach incident.

7.3.10. This report will then be provided to the Company's Board, the Chief Executive and the head of department whose department was impacted by the breach. All relevant risk registers must be updated in respect of the personal data/information

breach. Significant risks will be reported to both the Board and the Company's Audit and Finance Committee with matters addressed appropriately in line with the Company's Risk Management Policy

7.4. Notification

7.4.1. After taking the above into consideration, the IO and the other relevant members of the Company involved in the management of the breach, will determine whether or not it is necessary to notify the breach outside of the Company. Those that may need to be notified are:

7.4.1.1. The data subjects affected by the breach;

7.4.1.2. The shareholders/external funding organisations;

7.4.1.3. The IR (if the breach poses a risk to data/information subject/s);

7.4.1.4. The Police;

7.4.1.5. The press/media;

7.4.1.6. The Company's insurers;

7.4.2. If the breach may cause a risk to individuals, the breach must be reported to the IR.
When notifying the IR, as a minimum, the notification must include:

7.4.2.1. A description of how and when the personal data/information breach occurred;

7.4.2.2. What personal data/information was involved;

7.4.2.3. Who are the data/information subject involved;

7.4.2.4. Approximate number of personal data/information records concerned;

7.4.2.5. The likely consequences of the personal data/information breach; and

7.4.2.6. What action has been taken to respond to/resolve the risks posed by the breach.

7.4.3. Subject to certain exemptions, if the personal data/information breach causes, or is likely to cause, a high risk to the data subjects, it may be necessary to inform the data subjects. If it is deemed necessary to notify the data/information subject(s) of the breach, the IO must provide the data subjects in plain and clear language information on:

7.4.3.1. The name and contact details of the Company's IO or other point of contact;

7.4.3.2. The likely consequences of the personal data/information breach;

7.4.3.3. The measures taken or proposed to be taken by the Company to address the personal data/information breach, including where appropriate, measures to mitigate its possible adverse effects.

7.4.4. The IO must also decide on the most appropriate method of notification of the breach based on the following:

7.4.4.1. Are there a large number of data subjects involved;

7.4.4.2. Does the breach involve special category personal data/information;

7.4.4.3. Is it necessary to write to each individual affected;

7.4.4.4. Should legal advice be sought on the wording of the notification?

7.4.5. The IO must also ensure that the notification has a clear purpose e.g. that it enables the affected data subjects to take the necessary steps to protect themselves e.g. through cancelling bank cards, changing passwords etc., to allow regulatory bodies to perform their functions, provide advice and deal with any complaints. The focus of any breach response plan should be on protecting individuals and their personal data/information.

7.4.6. Timeframes

7.4.6.1. If the Company decides that it should (or if the IR determines that the Company must) inform the data subjects, this must be done without undue delay.

7.4.6.2. Where a decision is taken that it is necessary to notify the IR, this must be done by the IO within 72 hours from the point that the Company became aware of the incident. The Company will be regarded as having become "aware" when the Company has a reasonable degree of certainty that a security incident has occurred that has led to personal data/information being compromised. This will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish whether or not the personal data/information has been compromised.

7.4.6.3. Where precise information is not available (e.g. the exact number of data subjects affected) this should not be a barrier to timely breach notification. POPIA allows for approximations to be made in the number of individuals affected and the number of personal data/information records concerned as it recognises that controller/responsible party may not always have all details of the incident available during this initial period.

7.4.6.4. It is more likely this will be the case for more complex breaches, such as some cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach

and the extent to which personal data/information have been compromised.

7.4.6.5. Consequently, in some cases, the Company will have to do more investigation and follow-up with additional information at a later point. This is permissible as long as the Company provides reasoning for the delay. It should be noted that there is no penalty for reporting an incident that ultimately transpires to not be a breach.

7.4.6.6. The focus instead when reporting a breach should be directed towards addressing the adverse effects of the breach rather than providing precise figures of those affected. Thus, when it has become clear that there has been a breach, but the extent of it is not yet known, a notification in phases is a safe way to meet the notification obligations.

7.5. Evaluation and response

7.5.1. Subsequent to a personal data/information breach the IO, in consultation with the relevant members of the Company staff, will conduct a review to ensure that the steps taken during the incident were appropriate and to identify any areas for improvement.

7.5.2. The IO will report all data/information breaches to the Company's Board and the Executive Team, also maintaining a central record of all breach occurrences. However, for any serious breaches the IO will conduct a review and provide a detailed report to the Company Board and the Executive Team stating:

7.5.2.1. The action which needs to be taken to reduce the risk of future breaches to minimise their impact;

7.5.2.2. Whether any policies, procedures or reporting lines require improvement to increase the effectiveness of response to the breach;

7.5.2.3. If there are any faults or weak points in security controls which need to be tightened up;

7.5.2.4. Staff awareness/training issues which would prevent recurrence of the breach;

7.5.2.5. Additional investment in resources/infrastructure to reduce exposure to breach and relating cost implications.

7.5.3. It is important to keep in mind that, regardless of whether or not a breach needs to be notified, the Company must keep documentation of all breaches comprising the facts relating to the personal data/information breach, its effects and consequences and the remedial action that was taken. The Company will also record its reasoning for the decisions taken in response to a breach, in particular, if the breach has not been notified, a justification for that decision made. This documentation will enable the Company to verify its compliance. This is linked to the important accountability principle. If the Company fails to adequately document this process, there will be financial penalties.

8. POPIA COMPLIANCE

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

9. IMPLEMENTATION, MONITORING AND EVALUATION

9.1. The implementation, amendment, withdrawal, suspension and/ or revision of this policy is subject to the discretion of the Company.

9.2. Corporate Affairs Department is the custodian of this Policy.

9.3. Executive Management, Line Managers and Corporate Affairs Department are responsible for the implementation of the policy.

9.4. The Corporate Affairs Department will ensure there is effective monitoring of the policy.

9.5. Review of policies (including this policy) shall rest with the Executive Management and subsequent approval by the Board.

9.6. Policies are reviewed on a three (3) year basis and are to be reviewed in terms of best practice or as the need arises.

9.7. Any transgression of this policy shall be dealt with in accordance with the Company's disciplinary code & procedures and/or other relevant labour laws.

10. POLICY APPROVAL AND EFFECTIVE DATE

10.1. This policy is subject to the approval of the Board and shall take effect on the day subsequent to the approval date.

APPENDIX 1 - DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data/information security breaches. If you discover a data/information security breach, please notify your Head of Department immediately. Heads of Department should complete Section 1 of this form and email it to the Data/information Protection Officer as soon as practically possible. The Head of Department should also call the IO to ensure the IO has received the email.

SECTION 1:	
Notification of Data Security Breach	**To be completed by Head of Department of person reporting incident:**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data subjects affected, if known:	
Has any personal data/information been placed at risk? **If, so please provide details:**	
Brief description of any action taken at the time of discovery:	

NDALAMO OFFICE USE ONLY : TO BE COMPLETED BY IO	
Received by:	
Date Received:	
Forwarded for action to:	
Date Forwarded:	

SECTION 2: ASSESSMENT OF SEVERITY

Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data/information has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the firm or third parties?	
How many data subjects are affected?	
Is the data/information bound by any contractual security arrangements?	
HIGH RISK personal data/information	

• **Special Category Personal Data/information** (as defined in POPIA) relating to a living, identifiable individual's: o race; o ethnic origin; o politics; o religion; o trade union membership; o genetics; o biometrics (where used for ID purposes); o health; o sex life; or o sexual orientation • Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as National Insurance Number and copies of passports and visas; • Personal information relating to vulnerable adults and children; • Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; • Security information that would compromise the safety of individuals if disclosed. **Category of incident (0-6):** *(Refer to Annexure A)*	
Date Reported to Incident Manager:	
If level 3 or above: **Date escalated by IO to the Company's Executive Team**	

"ANNEXURE A"

DATA BREACH RATING

BREACH RATING	0 MINOR	1 LOW	2 HIGH	3 SERIOUS	4 SERIOUS	5 SERIOUS	6 SERIOUS
Ndalamo is Compromised	No significant impany on any individual or goupr of individuals	Damage to an individual's reputation or possible misuse of their personal data/information	Damamge to Ndalamo's reputation	Damage to more than one department within Ndalamo (reputation wise)	Damage to Ndalamo's reputation. Breach impacts on >20 but < 50 data subjects	Damage to Ndalamo's reputation. Breach impacts on >50 data subjects	Breach will carry monetary penalty from IR
	Media interest very unlikely	Media interest possible	Media interest possible but it may not penetrate the public domain	Possible key local media coverage	Local media coverage of breach	National media coverage	
Data subject is affected	Breach of confidentiality. Only a single data suject's information is affected	Breach is potentially serious but <10 data subjects affected and/or risk assessed as **LOW** e.g. files were encrypted	Potential serious breachand risk assessed as **HIGH** e.g. unencrypted special category records lost. Breach impacts on <50 data subjects	Breach of confidentiality e.g. up to 100 data subjects affected by e.g. loss of personal data relating to redundancies where data subjects are clearly identifiable	Breach with either particular sensitivity/ special category of personal information e.g. medical records or up to 1000 data subjects affected	Breach with potential for identity theft and/or 1000 data subjects affected	Restitution to affected data subjects. Other liabilities such as systems updates/new software. Additional systems/records Security. Legal Costs

** The preceding information serves as an overview of the potential severity of data breaches and the possible consequences that may arise from such incidents.*