Ndalamo Resources (Pty) Ltd
Living into The Future

PROTECTION OF PERSONAL INFORMATION POLICY

DOCUMENT TYPE	**ACCEPTABLE USE OF INFORMATION POLICY**	
DOCUMENT NO	**CORP AFF AUI: 14**	
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 AND SCOPE

2.1. The Company allows usage of information and technology for the sole purpose of enabling users to perform a specific job function. The Company expects users to handle and protect this information and technology appropriately, in a way that is acceptable to us.

2.2. This policy describes how information and technology is used. Use includes all forms of processing including accessing, using, storing or retrieving information. This policy also helps to:

2.2.1. Comply with the law, and

2.2.2. Protect the Company's reputation and intellectual property.

2.3. This policy implements good policies and processes to protect information and technology from threats and risks.

2.4. This policy applies to all users of the Company's information and technology, which includes:

2.4.1. Employees, temporary workers, contractors, stakeholders, and third parties who we allow to use our information (or technology), and

2.4.2. Our operators, who process personal information for us.

2.5. In addition, this policy applies to:

2.5.1. All information in physical and electronic form,

2.5.2. Information throughout its lifecycle (including its creation, collection, storage, distribution, archiving and disposal), and

2.5.3. All kinds of information, including personal information.

3. INFORMATION SECURITY PRINCIPLES

3.1. Confidentiality

3.1.1. Ensuring that confidentiality is not breached.

3.2. Integrity

3.2.1. Ensuring that the accuracy, completeness, and validity of information are not compromised.

3.3. Availability

3.3.1. Ensuring that the availability of technology and repositories are not impacted.

4. ROLES AND RESPONSIBILITIES

4.1. INFORMATION OFFICER (IO):

4.1.1. Implements and enforces Information Security policies and standards;

4.1.2. Formulates policies as and when required;

4.1.3. Designs and implements information security controls, commensurate with the risk appetite defined by business and in line with Operational Risk policies;

4.1.4. Advise information and system owners on security-related issues, architectures, and management;

4.1.5. Ensures that appropriate information security assessments are conducted and the appropriate remedial actions are implemented;

4.1.6. Ensures that this policy is fit for purpose and practical for implementation;

4.1.7. Maintains a database of exceptions (deviations or waivers) to the Information Security policies;

4.1.8. Provides oversight on the implementation of this policy;

4.1.9. Provides an independent view of information risk controls;

4.1.10. Gets vendors and operators to sign Non-Disclosure Agreements ("NDAs") and contracts (or Operator Agreements) before they start their engagements;

4.1.11. Represents a line of business for all information security matters;

4.1.12. Promotes awareness and monitor compliance with this policy;

4.1.13. Monitors policies and compliance;

4.1.14. Assists with the communication, implementation and management of our Information Security Programme;

4.1.15. Escalates information security incidents; and

4.1.16. Implements and enforces Information Security policies and standards.

4.2. EXECUTIVE MANAGEMENT:

4.2.1. Communicates and enforces compliance of this policy; and

4.2.2. Enforces the escalation of security incidents or response to incidents.

4.3. USERS:

4.3.1. Compliance with our approved IT security framework principles;

4.3.2. Compliance with this policy;

4.3.3. Uses authorised information only;

4.3.4. Reports security violations or non-compliance; and

4.3.5. Be vigilant and provides proactive information regarding the safeguarding of the Company's information.

5. ACCEPTABLE USE OF INFORMATION

5.1. INFORMATION ASSET MANAGEMENT

5.1.1. Users are advised to:

5.1.1.1. Protect and use information for authorised activities and permitted purposes in accordance with the information's classification level and handling requirements;

5.1.1.2. Treat all information as confidential. Protect the personal information of all parties, especially those that relate to the Company's customers and employees;

5.1.1.3. Return all the Company information when no longer authorised to use it (e.g., employment contract or engagement is terminated);

5.1.1.4. Protect the Company's information when removing it from the premises;

5.1.1.5. Protect the Company and each employee's intellectual property rights;

5.1.1.6. Protect the Company's information against any malicious activity and report any unacceptable activity;

5.1.1.7. Ensure that business continuity and disaster recovery capabilities are catered for in all information according to the Company's acceptable risks; and

5.1.1.8. Destroy obsolete information through formal channels (e.g. document shredding, degaussing etc.)

5.1.2. Users are advised not to:

5.1.2.1. Remove the Company's information from any laptops, desktops, or premises without authorisation.

5.1.2.2. Send or disclose any of the Company's information to third parties or unauthorised internal parties, unless authorised to do so.

5.1.2.3. Store customer data in any form other than authorised.

5.2. THIRD- PARTY SECURITY

5.2.1. Users are advised to:

5.2.1.1. Conduct an information security risk assessment when service contracts are agreed and signed with third parties;

5.2.1.2. Ensure that all third parties:

5.2.1.2.1. accept and understand all accountabilities and responsibilities related to the Company's information and technology; and

5.2.1.2.2. acknowledge the Company's security policies.

5.2.2. Users are advised not to:

5.2.2.1. Use third-party services without prior written approval (formal authorisation) from the respective executives and heads of department; and

5.2.2.2. Engage with third party vendors without:

5.2.2.2.1. Involving the necessary Head of Department; and

5.2.2.2.2. A contract, which should include a confidentiality clause.

5.3. INFORMATION SECURITY INCIDENT MANAGEMENT

5.3.1. Users are advised to:

5.3.1.1. Report information security incidents to IT, their line manager and IO immediately when information is:

5.3.1.1.1. Downloaded to USBs;

5.3.1.1.2. Accessed without authorisation; or

5.3.1.1.3. Otherwise downloaded.

5.3.1.2. Escalate to line management if uncertain on how to handle or deal with information security incidents.

5.4. NETWORK AND IT OPERATIONS SECURITY

5.4.1. Users are advised to:

5.4.1.1. Immediately report any software malfunction to line management and IT.

5.4.2. Users are advised not to:

5.4.2.1. Use private, personally owned or any device not owned by the Company to access the Company's network or information unless approved by management. Do not plug cellular phones into laptops for charging or use personal USBs;

5.4.2.2. Tamper with, disable or modify any of the Company's approved software and information security controls;

5.4.2.3. Use unsecured wireless access to connect to the Company's technology;

5.4.2.4. Use software that is able to scan or interrogate the Company's technology, unless specifically authorised to do so as part of the user's job responsibilities; and

5.4.2.5. Use any unauthorised USB devices.

5.5. LOGICAL ACCESS MANAGEMENT

5.5.1. Users are advised to:

5.5.1.1. Correctly complete a request for access form and get approval from their line manager. Remove access for former employees and internal transfers;

5.5.1.2. Keep passwords secure and do not share them with anyone, even IT or line manager. Users will be held accountable for any unauthorised actions performed with the user's own account;

5.5.1.3. If users think someone is aware of their password, or it has been compromised, change it immediately and report the incident to their line manager;

5.5.1.4. Ensure all devices are password protected (e.g. a company USB used to access, process, store or transmit our information);

5.5.1.5. If users work from any of the Company's locations (owned, rented or leased), users must ensure that the information and computer used is adequately protected and cannot be accessed by unauthorised people; and

5.5.1.6. Make use of complex passwords containing alphanumerical characters.

5.5.2. Users are advised not to:

5.5.2.1. Access any technology unless authorised to do so; and

5.5.2.2. Access any unauthorised information.

5.6. CLEAN DESK

5.6.1. Refer to Clear Dear and Clear Screen Policy.

5.7. APPROVED SOFTWARE

5.7.1. Users are advised to:

5.7.1.1. Use the Company's licensed and approved software on all the Company's technology.

5.7.2. Users are advised not to:

5.7.2.1. Install unapproved software on any of the Company's computers or devices.

5.8. ENCRYPTION

5.8.1. Users are advised to:

5.8.1.1. Consult guidelines for the use of encryption tools or devices when relevant and obtain authorisation for encryption.

5.8.2. Users are advised not to:

5.8.2.1. Encrypt any of the Company's information using software or tools that have not been approved by IT or the Company's Information Security; and

5.8.2.2. Perform any unauthorised cryptographic activities (e.g. encrypt or decrypt).

5.9. RISK ASSESSMENT

5.9.1. Users are advised to:

5.9.1.1. Report risks to the line manager or IO.

5.9.2. Users are advised not to:

5.9.2.1. Discuss risks with unauthorised parties; and

5.9.2.2. Ignore any risks or risk escalation.

5.10. INFORMATION SECURITY (IS) COMPLIANCE

5.10.1. Users are advised to:

5.10.1.1. Adhere to copyright laws;

5.10.1.2. Protect personal information;

5.10.1.3. Retain information in accordance with defined policies, standards, legal or regulatory obligations; and

5.10.1.4. Adhere to all regulations that are applicable.

5.11. HUMAN RESOURCES

5.11.1. Users are advised to:

5.11.1.1. Adhere to information security principles.

5.11.1.2. Return all information before leaving the Company. If moving within the Company, users must get approval from the head of the department to retain any information; and

5.11.1.3. Ensure that the user's Human Resources records are updated when their job role changes.

5.12. PHYSICAL SECURITY

5.12.1. Users are advised not to:

5.12.1.1. Remove any IT equipment from the Company's premises without prior approval and without following the physical security processes.

5.13. PRIVACY

5.13.1. Users are advised to:

5.13.1.1. Protect and use personal information in accordance with the Company's privacy requirements and all laws and regulations;

5.13.1.2. The Company reserves the right to intercept, monitor, block, access, retrieve, read, or disclose user information or indirect communications whilst conducting its normal business activities; and

5.13.1.3. The Company owns all its information and technology.

5.13.2. Users are advised not to:

5.13.2.1. Send any personal information or customer information to third parties unless authorised by management or the information owner; and

5.13.2.2. Send private emails.

5.14. BUSINESS CONTINUITY MANAGEMENT

5.14.1. Users are advised to:

5.14.1.1. Regularly backup business information on the network drive or alternative approved storage. Be aware of space implications; and

5.14.1.2. Adhere to business continuity requirements.

5.15. EMAIL USAGE, INTERNET USAGE, AND ELECTRONIC COMMUNICATION

5.15.1. Users are advised to:

5.15.1.1. Use the Company's communication technology in a responsible, ethical and secure manner; and

5.15.1.2. When sending an email, users are acting on the Company's behalf. Users must always portray a professional image at all times.

5.15.2. Users are advised not to:

5.15.2.1. Send or forward the Company's information or customer information to personal or private email accounts;

5.15.2.2. Send the Company's information to web-based email addresses (E.g. Gmail), unless it is for legitimate business reasons that have been approved by the line manager;

5.15.2.3. Automatically forward email to an external email account;

5.15.2.4. Use web-based email accounts (like Gmail) on the Company's equipment or personal devices connected to the Company's network;

5.15.2.5. Use the Company's email, Internet and intranet facilities to access, download or distribute pornography, games, inappropriate graphics or files, illegal software or for gambling or for playing games;

5.15.2.6. Use the Company's email, Internet and intranet facilities for unacceptable activities. Unacceptable activities include, but is not limited to;

5.15.2.6.1. Fraud;

5.15.2.6.2. Harassment;

5.15.2.6.3. Life threats;

5.15.2.6.4. Defamation;

5.15.2.6.5. Sexually explicit content;

5.15.2.6.6. Intimidation;

5.15.2.6.7. Maliciousness, or

5.15.2.6.8. Racism, hate, or obscenities.

5.15.2.7. Use the Company's email, Internet and electronic facilities for selling or marketing anything private (or any other business activities other than the Company's);

5.15.2.8. Use the Company's technology in a manner that adversely affects users productivity or the availability of the Company's information; and

5.15.2.9. Email customer data.

5.16. INTELLECTUAL PROPERTY

5.16.1. Users are advised to:

5.16.1.1. Use material (products, software, or information) covered by intellectual property rights in-line with legislative, regulatory and contractual requirements.

5.16.1.2. Accept that all intellectual property created during users employment is the Company's property and must be protected.

5.17. FILE- SHARING

5.17.1. Users are advised to:

5.17.1.1. Adhere to control principles when creating file shares. Ensure that Information Technology (IT) has created or assigned it to authorised employees only; and

5.17.1.2. Store the Company's (or customer or any third-party) information on designated file servers or network drives and not on local drives on users computers.

5.17.2. Users are advised not to:

5.17.2.1. Share data on a network or give anyone access to their computer;

5.17.2.2. Access or copy unauthorised or copyrighted material as this is illegal. This includes books, music and movies. Do not copy this information off the Internet or from a computer or memory device;

5.17.2.3. Download any illegal software on to their computer;

5.17.2.4. Share information or technology that are important to the Company, with unauthorised employees and third parties. If unsure whether information is sensitive or personal, ask the line manager for guidance. Certain documents could have a security classification; and

5.17.2.5. Connect to any unsecured non-company network from work computers or laptops, as this is a security risk.

5.18. SOCIAL NETWORKING

5.18.1. Users are advised not to:

5.18.1.1. Disclose the Company (or third-party's) confidential or proprietary information without proper authorisation when blogging or using social media platforms;

5.18.1.2. Engage in any blogging or social media activity that may harm or damage the Company's image, reputation or goodwill or any of the Company's employees; and

5.18.1.3. Post comments that are obscene, insulting, derogatory, sexist, racist, homophobic and offensive to colleagues, management or any other person or entity.

6. EXCEPTIONS

6.1. There are no exceptions to this policy, unless the Company has authorised in writing to use information in any manner otherwise.

7. POPIA COMPLIANCE

7.1. 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.

8. IMPLEMENTATION, MONITORING AND EVALUATION

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

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

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

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

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

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

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

9. POLICY APPROVAL AND EFFECTIVE DATE

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