



**POLICY**

**PRIVACY**

Revision Number:	6.0
Classification:	Public
Draft <input type="checkbox"/> /Final <input checked="" type="checkbox"/> as of:	22 February 2024
Document Owner:	Chief Legal and Compliance Officer
Contact Tel:	+27 010 900 2442

**Route Monitoring (RF) (PTY) LTD**  
**178 Cumberland Avenue**  
**Turnberry Office Park**  
**Bryanston**  
**2191**

## Disclaimer and Copyright Notice

Copyright © 2024, Route Monitoring (RF) (Pty) Ltd. All Rights Reserved.

No parts of this work may be reproduced in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the written permission of Route Monitoring (RF) (Pty) Ltd. Products that are referred to in this document may be either copyrights or trademarks of the respective owners. The publisher and/or the author make no claim with regard to such copyrights or trademarks. While every precaution has been taken in the preparation of this document, the publisher and/or the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programmes and/or source codes that may accompany it. In no event shall the publisher and/or the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document. Changes to this document will be made in accordance to the Document Management Policy and Procedure and previous revisions of the document will no longer be valid.

## Content Revision History

Date	Revision Number	Author	Comments – Note sections that changed
01 June 2021	1.0	Legal and Compliance Associate	1 <sup>st</sup> Draft created 12 May 2021. Reviewed, amended and approved by L&C Manager and Chief Legal and Compliance Officer.
21 June 2021	2.0	Legal and Compliance Manager	Updated Reference Documents to include all documents which deal with Personal Information. Added 4.28 (ref docs to be regularly updated).
28 June 2021	3.0	Legal and Compliance Associate	Included clauses relating to “Personal Information disclosure to suppliers” (4.15) and “Transborder Information Flows” (4.16). Updated reference documents to include New Equipment Procurement Procedure; Managed Services Support Procedure; TEC-PL_Appendix 3_List of Business Continuity Sites; TEC-PL_Appendix 5_Key Contacts and Bank Accounts Procedure.

22 February 2022	4.0	Legal and Compliance Associate	Annual review. Added Service Provider / Supplier to Glossary of Terms. Amended clause 4.13.1.5 by replacing "its local data protection authority" with "Information Regulator".
22 February 2023	5.0	Legal and Compliance Manager	<p>Annual review:</p> <ul style="list-style-type: none"> <li>- Removed "TEC-PR_Managed Services Support Procedure" and Covid-19 documents from reference docs as they were archived</li> <li>- Updated breach clause and formatting as per update document management template</li> <li>- Amended 4.30 to refine the heading and contents thereof (updates to reference documents)</li> <li>- Updated TOC</li> <li>- Updated expired links in the reference docs</li> <li>- Amended names of Information Classification Policy, Clear Desk and Clear Screen Policy and IT Security Policy due to change from "TEC" to "OP" (in ref docs and in clause 4.12.6).</li> </ul>

22 February 2024	6.0	Legal and Compliance Associate	<p>Annual Review:</p> <ul style="list-style-type: none"> <li>- Updated expired LC-POL_Privacy Policy link under clause 4.29.2.1.</li> <li>- Updated following expired links under clause 6 - Reference Documents: CEO-MN_PAIA and POPI Manual, CEO-POL_Information Security Policy, CEO-POL_Change Management Policy, CEO-PR_Change Management Procedure, and CS-PR_Risk Management Procedure.</li> <li>- Added LC-POL_Compliance Policy and LC-POL Regulator Liaison Policy as reference documents.</li> </ul>
------------------	-----	--------------------------------	---

**RACI Model**

Responsible	Accountable	Consulted	Informed
Legal and Compliance Manager	Chief Legal and Compliance Officer	All HODs	All RM Staff
Legal and Compliance Associate			
All Staff			

## TABLE OF CONTENTS

1.	GLOSSARY OF TERMS .....	8
2.	PURPOSE .....	10
3.	SCOPE.....	10
4.	POLICY .....	10
4.1	Objectives.....	10
4.2	Processing Conditions .....	11
4.3	Accountability (Condition 1) .....	11
4.4	Processing Limitation (Condition 2) .....	11
4.5	Purpose Specification (Condition 3).....	12
4.6	Further Processing Limitation (Condition 4) .....	12
4.7	Information Quality (Condition 5) .....	12
4.8	Openness (Condition 6) .....	12
4.9	Security Safeguards (Condition 7) .....	13
4.10	Data Subject Participation (Condition 8) .....	13
4.11	Processing of the Personal Information collected .....	13
4.12	Protecting the Data Subject's Personal Information .....	15
4.13	The Data Subject's rights regarding its Personal Information .....	15
4.14	Processing of Special Personal Information .....	16
4.15	Personal Information disclosure to Service Provider / Suppliers .....	17
4.16	Transborder Information Flows .....	17
4.17	Destruction and Retention of Personal Information and Documents .....	17
4.18	Retention in terms of the Companies Act, 2008 (Act No. 71 of 2008) .....	17
4.19	Retention in terms of the Electronic Communication and Transaction Act, 2002 (Act No. 25 of 2002) .....	18
4.20	Retention in terms of the Compensation for Occupational Injuries and Diseases Act, 1993 (Act No. 130 of 1993) .....	18
4.21	Retention in terms of the Occupational Health and Safety Act, 1993 (Act No. 85 of 1993) .....	19
4.22	Retention in terms of the Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997) .....	19
4.23	Retention in terms of the Employment Equity Act, 1998 (Act No. 55 of 1998) .....	19
4.24	Retention in terms of the Labour Relations Act, 1995 (Act No. 66 of 1995) .....	19
4.25	Retention in terms of the Unemployment Insurance Act, 2001 (Act No. 63 of 2001) .....	20
4.26	Retention in terms of the Tax Administration Act, 2011 (Act No. 28 of 2011) .....	20
4.27	Retention in terms of the Income Tax Act, 1962 (Act No. 58 of 1962) .....	20
4.28	Retention in terms of the Value Added Tax Act, 1991 (Act No. 89 of 1991) .....	20

4.29	Route Monitoring Disclaimers .....	21
4.30	Reference documents to be regularly updated .....	21
4.31	Breach .....	21
5.	REVIEW .....	22
6.	REFERENCE DOCUMENTS .....	22

## 1. GLOSSARY OF TERMS

Data Subject	Means the person to whom Personal Information relates.
Information Officer	Means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
Limited Pay-Out Machine ("LPM")	a gambling machine with a restricted prize [NCEMS Service Level Contract]
National Central Electronic Monitoring System or Evolution ("NCEMS")	Referred to in section 27 of the NGA is to be implemented for the detection and monitoring of significant events associated with any LPM that is made available for play in the RSA and for analysing and reporting the detected data in accordance with the requirements of the NGA [NCEMS Service Level Contract]
National Gambling Board ("NGB")	Is the National Gambling Board of South Africa constituted in terms of National Gambling Act (Act no 7 of 2004) and is a Schedule 3A listed Public Entity in terms of the Public Finance Management Act (Act no 1 of 1999) as amended from time to time [NCEMS Service Level Contract]
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, wellbeing, 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;



	<p>(c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;</p> <p>(d) the biometric information of the person;</p> <p>(e) the personal opinions, views or preferences of the person;</p> <p>(f) (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;</p> <p>(g) the views or opinions of another individual about the person; and</p> <p>(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.</p> <p>[Protection of Personal Information Act, 2013 (Act No. 4 of 2013)]</p>
POPI Act	Protection of Personal Information Act (Act 4 of 2013)
Route Monitoring ("RM")	Is Route Monitoring (RF) (PTY) Limited constituted in terms of the Companies Act, Act no. 71 of 2008 as amended from time to time.
Service Provider / Supplier	<p>any natural or Juristic person which has been contracted for the supply of goods or services</p> <p>[NCEMS Service Level Contract]</p>
Service Level Contract ("SLC")	Refers to the "NCEMS Service Level Contract" entered into between the NGB and Route Monitoring on the 11th of September 2017

## 2. PURPOSE

RM is the NCEMS Operator, monitoring all LPMs within the South African gambling industry on behalf of the NGB.

RM collects and uses Personal Information of Data Subjects it interacts with in order to operate and carry out its business effectively. RM regards the lawful and appropriate processing of all Personal Information as crucial to accurate and prompt service delivery and essential to maintaining confidence between itself and Data Subjects. RM therefore fully endorses and adheres to the principles of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) [as amended].

The purpose of this Policy is to define clear rules and methods on how RM will meet its legal obligations and requirements relating to the use of Personal Information as more fully set out in the POPI Act and any ancillary regulations, codes, legislation, rules, etc.

## 3. SCOPE

This Policy is applicable to all RM's Data Subjects including permanent and contracted employees, customers, consultants, service providers / suppliers, operators, regulators, shareholders, directors, sub-contractors and agents, as well as all external parties who conduct business with RM.

## 4. POLICY

### 4.1 Objectives

- 4.1.1 To give effect to the POPI Act.
- 4.1.2 To document the eight conditions of lawful processing of Personal Information as contained in the POPI Act for implementation thereof.
- 4.1.3 To strive to take appropriate, reasonable, technical and organizational measures to secure the integrity and confidentiality of Personal Information in RM's possession or under its control.
- 4.1.4 To clarify what Personal Information RM collects and the purpose of the processing of the Personal Information collected in relation to Data Subjects.
- 4.1.5 To clarify how RM uses and protects the Personal Information of a Data Subject.
- 4.1.6 To stipulate the rights of a Data Subject in relation to their Personal Information.
- 4.1.7 To define retention periods for Personal Information and provide for the destruction of same after respective retention period(s) have lapsed.

## 4.2 Processing Conditions

4.2.1 Processing for purposes of this Policy is defined to mean any operation or activity or any set of operations, whether or not by automatic means, concerning Personal information, including:

- 4.2.1.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- 4.2.1.2 dissemination by means of transmission, distribution or making available in any other form; or
- 4.2.1.3 merging, linking, as well as restriction, degradation, erasure or destruction of information.

4.2.2 The POPI Act requires Personal Information to be processed in accordance with eight lawful processing conditions. RM shall abide by such conditions in all its processing activities.

## 4.3 Accountability (Condition 1)

4.3.1 RM shall ensure that all processing conditions, as set out in the POPI Act, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing of the Personal Information, as well as during the processing itself.

## 4.4 Processing Limitation (Condition 2)

4.4.1 Personal Information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject.

4.4.2 Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

4.4.3 RM may only process Personal Information if:

- 4.4.3.1 The Data Subject (or a person who has been given authorisation by the Data Subject to provide the Data Subject's Personal Information) consents to such processing;
- 4.4.3.2 The Processing is necessary for the conclusion or performance of a contract;
- 4.4.3.3 The Processing complies with a legal responsibility imposed on RM;
- 4.4.3.4 The Processing protects a legitimate interest of the Data Subject;
- 4.4.3.5 The Processing is necessary for the pursuance of a legitimate interest of RM or a third party to whom the information is supplied.

4.4.4 Personal Information must be collected directly from the Data Subject, unless:

- 4.4.4.1 The Data Subject consents to collection of information from another source;
- 4.4.4.2 Personal Information is contained in a public record or has been deliberately made public by

the Data Subject;

- 4.4.4.3 Personal Information is collected from another source with the Data Subject's consent;
- 4.4.4.4 Collection of Personal Information from another source would not prejudice the Data Subject;
- 4.4.4.5 Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
- 4.4.4.6 Collection from the Data Subject would prejudice the lawful purpose of collection;
- 4.4.4.7 Collection from the Data Subject is not reasonably practicable.

#### 4.5 Purpose Specification (Condition 3)

- 4.5.1 Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of RM.
- 4.5.2 Records of Personal Information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or processed for.

#### 4.6 Further Processing Limitation (Condition 4)

- 4.6.1 Further processing of Personal Information must be in accordance or compatible with the original purpose of processing.
- 4.6.2 Further processing will be regarded as compatible with the purpose of collection if:
  - 4.6.2.1 The Data Subject (or a person who has been given authorisation by the Data Subject to provide the Data Subject's Personal Information) has consented to the further processing;
  - 4.6.2.2 Personal Information is contained in a public record or has been deliberately made public by the Data Subject;
  - 4.6.2.3 Further processing is necessary to maintain, comply with or exercise any law or legal right;
  - 4.6.2.4 Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party;
  - 4.6.2.5 The information is used for historical, statistical or research purposes.

#### 4.7 Information Quality (Condition 5)

- 4.7.1 RM shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated.

#### 4.8 Openness (Condition 6)

- 4.8.1 RM shall maintain the documentation of all processing operations under its responsibility in accordance with the CEO-MN\_PAIA and POPI Manual.
- 4.8.2 RM shall take reasonable steps to ensure that the Data Subject is made aware of:
  - 4.8.2.1 What Personal Information is collected and / or the source from which the information is collected from;
  - 4.8.2.2 The name and address of RM;
  - 4.8.2.3 The purpose for which the information is being collected and processed for;
  - 4.8.2.4 Whether the supply of Personal Information is voluntary or mandatory;
  - 4.8.2.5 Consequences of a failure to provide the information;
  - 4.8.2.6 Whether collection is in terms of any law requiring such collection;
  - 4.8.2.7 Whether the Personal Information shall be transferred to a third party, another country or an international organisation and the level of protection afforded to the information by that third party, country or international organisation;
  - 4.8.2.8 Nature of the information being collected and processed;
  - 4.8.2.9 The rights of the Data Subject.
- 4.9 Security Safeguards (Condition 7)
  - 4.9.1 RM shall ensure the integrity and confidentiality of all Personal Information in its possession or under its control.
  - 4.9.2 RM shall take appropriate and reasonable measures to prevent the loss of, damage to, or unauthorised destruction of Personal Information, as well as to prevent the unlawful access to or processing of Personal Information.
  - 4.9.3 RM shall identify all reasonably foreseeable internal and external risks to Personal Information and establish and maintain appropriate and updated safeguards against such risks in accordance with the CS-POL\_Risk Management Policy and CS-PR\_Risk Management Procedure.
- 4.10 Data Subject Participation (Condition 8)
  - 4.10.1 A Data Subject has the right to request access to, amendment of, or deletion of their Personal Information. All such requests must be submitted in writing to the Information Officer and in accordance with the CEO-MN\_PAIA and POPI Manual.
- 4.11 Processing of the Personal Information collected

- 4.11.1 The categories of Data Subjects as well as the categories of Personal Information which RM processes is contained in the CEO-MN\_PAIA and POPI Manual.
- 4.11.2 Further, the categories of recipients to whom the Personal Information may be supplied to is similarly contained in the CEO-MN\_PAIA and POPI Manual.
- 4.11.3 The purpose for which Personal Information is processed by RM will depend on the nature of the information and the purpose for which it was collected. This may include:
  - 4.11.3.1 Only information that is adequate, necessary and relevant;
  - 4.11.3.2 Providing products or services to Data Subjects and to carry out the transactions requested;
  - 4.11.3.3 To carry out actions for the conclusion or performance of a contract;
  - 4.11.3.4 Conducting credit reference searches or verifications;
  - 4.11.3.5 Confirming, verifying and updating Data Subjects' details as well as Data Subject administration;
  - 4.11.3.6 For the detection and prevention of fraud, crime, money laundering or other malpractices;
  - 4.11.3.7 Conducting market or customer satisfaction research;
  - 4.11.3.8 For audit and record keeping purposes;
  - 4.11.3.9 In connection with legal proceedings;
  - 4.11.3.10 To maintain the relationship between RM and its Data Subjects;
  - 4.11.3.11 Providing communication in respect of RM and regulatory matters that may affect the Data Subjects;
  - 4.11.3.12 In complying with legal and regulatory duties and obligations;
  - 4.11.3.13 For debt recovery;
  - 4.11.3.14 Electronic communication sent to RM by a Data Subject;
  - 4.11.3.15 Information submitted to RM by a Data Subject;
  - 4.11.3.16 Information when a Data Subject completes certain "User Forms" and submits same to the RM's Helpdesk for specific access rights and/or similar purposes as further detailed in the OP-POL\_Helpdesk Policy and OP-PR\_Helpdesk Procedure;
  - 4.11.3.17 Information when a Data Subject completes a form on the RM website;
  - 4.11.3.18 To protect the legitimate interests of the Data Subjects; and
  - 4.11.3.19 Where it is necessary for pursuing the legitimate interests of the Company.

#### 4.12 Protecting the Data Subject's Personal Information

- 4.12.1 It is a requirement of the POPI Act to adequately protect Personal Information and prevent unauthorised access to a Data Subject's Personal Information. RM will continuously review its information security policies and procedures to ensure that a Data Subject's information is secure.
- 4.12.2 RM's Information Officer and Deputy Information Officers are responsible for the compliance with the conditions of the lawful processing of Personal Information and other provisions of the POPI Act. RM's Information Officers and Deputy Information Officers are detailed in the CEO-MN\_PAIA and POPI Manual.
- 4.12.3 Consent to process a Data Subject's information must be obtained from the Data Subject (or a person who has been given authorisation by the Data Subject to provide their Personal Information).
- 4.12.4 Every new employee will be provided with this LC-POL\_Privacy Policy and relevant related documentation to alert them to the measures in place to protect their Personal Information.
- 4.12.5 Personal Information which is no longer required should be disposed of by shredding.
- 4.12.6 The OP-POL\_Clear Desk and Clear Screen Policy, OP-POL\_Information Classification Policy, and the OP-POL\_IT Security Policy should be maintained and adhered to at all times.
- 4.12.7 All electronically held Personal Information should be saved on a secure database.
- 4.12.8 All electronically held Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.
- 4.12.9 Unauthorised access to Personal Information and Breach Notifications
- 4.12.10 Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Deputy Information Officers, who shall notify the Information Officer and the Technical department, who shall take all necessary steps to remotely delete the information, if possible.
- 4.12.11 Where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person, RM must immediately notify —
  - 4.12.11.1 the Information Regulator; and
  - 4.12.11.2 the Data Subject, unless the Information Regulator determines that such notification will impede a criminal investigation by the public body concerned.

#### 4.13 The Data Subject's rights regarding its Personal Information

LC-POL_Privacy Policy	
Copyright © Route Monitoring (RF) (Pty) Ltd 2024. All Rights Reserved.	Page 15 of 25

4.13.1 The Data Subject is entitled to:

- 4.13.1.1 Request RM for access to the Personal Information it has on record for it;
- 4.13.1.2 Request the updating, correction and/or deletion of it's Personal Information;
- 4.13.1.3 Request the restriction of the processing of its Personal Information, or object to that processing;
- 4.13.1.4 Refuse or withdraw its consent to the processing of its Personal Information as well as object to the processing of its Personal Information at any time unless legislation provides for such processing. Once a data subject withdraws its consent or objects to the processing of its information then RM shall refrain from processing the Personal Information;
- 4.13.1.5 Complain to Information Regulator where it is believed that it's privacy rights are violated or it has suffered as a result of unlawful processing of it's Personal Information.

4.14 Processing of Special Personal Information

4.14.1 Special Personal Information includes:

- 4.14.1.1 Religious, philosophical, or political beliefs;
- 4.14.1.2 Race or ethnic origin;
- 4.14.1.3 Trade union membership;
- 4.14.1.4 Health or sex life;
- 4.14.1.5 Biometric information
- 4.14.1.6 Criminal behaviour;
- 4.14.1.7 Information concerning a child.

4.14.2 RM may only process Special Personal Information under the following circumstances:

- 4.14.2.1 The Data Subject has consented to such processing;
- 4.14.2.2 The Special Personal Information was deliberately made public by the Data Subject;
- 4.14.2.3 Processing is necessary to comply with an obligation of international public law;
- 4.14.2.4 Processing is necessary for the establishment of a right or defence in law;
- 4.14.2.5 Processing is for historical, statistical, or research purposes to the extent that the purpose will serve a public interest or would involve an impossible or disproportionate effort for consent;
- 4.14.2.6 The processing of race or ethnic origin is in order to comply with B-BBEE and Employment Equity (affirmative action) laws.



#### 4.15 Personal Information disclosure to Service Provider / Suppliers

4.15.1 RM may share Personal Information with its suppliers and service providers as needed to deliver products or services to its Data Subjects.

4.15.2 RM concludes Non-Disclosure Agreements with all Service Providers / Suppliers where information disclosure may be required in accordance with the LC-POL\_Supplier Security Policy.

#### 4.16 Transborder Information Flows

4.16.1 Personal Information may be transferred cross-border to RM's authorised third-party service providers and Personal Information may be stored in data servers hosted outside of South Africa. RM ensures that such third-party service providers protect its personal information with measures as protective as the laws in South Africa. RM will endeavour to ensure that its third-party service providers make all reasonable efforts to secure Personal Information and will implement appropriate and reasonable measures to ensure that the Personal information of its Data subject remains protected and secure when it is transferred outside South Africa.

#### 4.17 Destruction and Retention of Personal Information and Documents

4.17.1 Records of Personal Information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed for, unless –

4.17.1.1 retention of the record is required or authorised by law;

4.17.1.2 retention of the record is required by a contract between the parties thereto; or

4.17.1.3 the data subject or a competent person where the Data Subject is a child has consented to the retention of the record.

4.17.2 RM shall only retain Personal Information of Data Subjects for longer periods for historical, statistical and research purposes.

4.17.3 Documents may be destroyed after the lapsing of the retention period specified herein, or as determined by the Company from time to time.

4.17.4 Any Personal Information not covered by a specific retention period contained in the legislation identified herein below will have a general retention period equal to the duration of the SLC entered into between RM and the NGB.

#### 4.18 Retention in terms of the Companies Act, 2008 (Act No. 71 of 2008)

4.18.1 Hardcopies of the documents mentioned below must be retained for 7 years:

4.18.1.1 Any documents, accounts, books, writing, records or other information that a company is

required to keep in terms of the Act;

4.18.1.2 Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities;

4.18.1.3 Copies of reports presented at the annual general meeting of the company;

4.18.1.4 Copies of annual financial statements required by the Act;

4.18.1.5 Copies of accounting records as required by the Act;

4.18.1.6 Record of directors and past directors, after the director has retired from the company;

4.18.1.7 Written communication to holders of securities; and

4.18.1.8 Minutes and resolutions of directors' meetings, audit committee and directors' committees.

4.18.2 Copies of the documents mentioned below must be retained indefinitely:

4.18.2.1 Registration certificate;

4.18.2.2 Memorandum of Incorporation and alterations and amendments;

4.18.2.3 Rules;

4.18.2.4 Securities register and uncertified securities register;

4.18.2.5 Register of company secretary and auditors; and

4.18.2.6 Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply)

4.18.2.7 Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

4.19 Retention in terms of the Electronic Communication and Transaction Act, 2002 (Act No. 25 of 2002)

4.19.1 Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information as long as the information is used, and at least 1 year thereafter.

4.19.2 A record of any third party to whom the information was disclosed must be kept for as long as the information is used and at least 1 year.

4.19.3 All personal data which has become obsolete must be destroyed.

4.20 Retention in terms of the Compensation for Occupational Injuries and Diseases Act, 1993 (Act No. 130 of 1993)

4.20.1 A retention period of 4 years is required for the documents mentioned below:

4.20.1.1 Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.

4.21 Retention in terms of the Occupational Health and Safety Act, 1993 (Act No. 85 of 1993)

4.21.1 A retention period of 3 years is required for the documents mentioned below:

4.21.1.1 Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;

4.21.1.2 Records of incidents reported at work.

4.22 Retention in terms of the Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997)

4.22.1 A retention period of 3 years is required for the documents mentioned below:

4.22.1.1 Written particulars of an employee after termination of employment;

4.22.1.2 Employee's name and occupation;

4.22.1.3 Time worked by each employee;

4.22.1.4 Remuneration paid to each employee;

4.22.1.5 Date of birth of any employee under the age of 18 years.

4.23 Retention in terms of the Employment Equity Act, 1998 (Act No. 55 of 1998)

4.23.1 A retention period of 3 years is required for the documents mentioned below:

4.23.1.1 Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;

4.23.1.2 The report which is sent to the Director General as indicated in the Act.

4.24 Retention in terms of the Labour Relations Act, 1995 (Act No. 66 of 1995)

4.24.1 A retention period of 3 years is required for the documents mentioned below:

4.24.1.1 Records to be retained by the employer are the collective agreements and arbitration awards.

4.24.2 An indefinite retention period is required for the documents mentioned below:

4.24.2.1 An employer must retain prescribed details of any strike, lock-out or protest action involving its employees;

4.24.2.2 Records of each employee specifying the nature of any disciplinary transgressions, the actions

taken by the employer and the reasons for the actions.

#### 4.25 Retention in terms of the Unemployment Insurance Act, 2001 (Act No. 63 of 2001)

4.25.1 Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed for a period of 5 years.

#### 4.26 Retention in terms of the Tax Administration Act, 2011 (Act No. 28 of 2011)

4.26.1 A retention period of 5 years is required for all documents contained in section 29 of the Tax Administration Act which:

4.26.1.1 Will enable a person to observe the requirements of the Act;

4.26.1.2 Are specifically required under a Tax Act by the Commissioner by the public notice;

4.26.1.3 Will enable SARS to be satisfied that the person has observed these requirements.

#### 4.27 Retention in terms of the Income Tax Act, 1962 (Act No. 58 of 1962)

4.27.1 A retention period of 5 years is required with regards to the following information:

4.27.1.1 The Amount of remuneration paid or due by the employer to the employee;

4.27.1.2 The amount of employees' tax deducted or withheld from the remuneration paid or due;

4.27.1.3 The income tax reference number of an employee;

4.27.1.4 Any further prescribed information;

4.27.1.5 Employer's Reconciliation return.

#### 4.28 Retention in terms of the Value Added Tax Act, 1991 (Act No. 89 of 1991)

4.28.1 A retention period of 5 years is required from the date of submission of the return for the documents mentioned below:

4.28.1.1 Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;

4.28.1.2 Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;

4.28.1.3 Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques;

4.28.1.4 Documentary proof substantiating the zero rating of supplies;

4.28.1.5 Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.

#### 4.29 Route Monitoring Disclaimers

4.29.1 All external documents and or forms may contain a link to RM's Disclaimers, which can be found on the RM's website: [Website Disclaimer - Route Monitoring](#).

4.29.2 Further, all external documents and / or forms where personal information will be processed must contain the following disclaimer:

4.29.2.1 "All personal information submitted herein shall solely be used for the specific, explicitly defined and lawful purpose relating to a function or activity of Route Monitoring. Route Monitoring takes the protection of your personal information very seriously. We treat your personal information as confidential and in accordance with the POPI Act and the [LC-POL Privacy Policy](#). Route Monitoring undertakes to ensure that appropriate security controls measures are implemented to protect any and all personal information submitted by a data subject to Route Monitoring. However, full protection of your personal data / information from unauthorised third-party access is not guaranteed albeit very strict information security controls which are in place and continuously monitored. Route Monitoring assumes that once a data subject submits personal information for the purposes of processing same, that the personal information is submitted in good faith and with the required consent to process same. Route Monitoring does however not make any warranties about the completeness, reliability and accuracy of the personal information submitted by a data subject. Any action you take upon the information provided, is strictly at your own risk and Route Monitoring will not be liable for any losses and/or damage suffered in connection with the submitting of this personal information."

#### 4.30 Reference documents to be regularly updated

4.30.1 All operational documents related to personal information are cited in the reference documents in section 6. hereinbelow and will be continuously and regularly updated.

#### 4.31 Breach

4.31.1 Breach of this Policy may lead to disciplinary action in terms of the CS-POL\_Disciplinary Policy and CS-PR\_Disciplinary Procedure.

## 5. REVIEW

This LC-POL\_Privacy Policy must be reviewed, at minimum, annually and as and when required or when RM experiences structural changes which significantly affect the organisational structure.

RM reserves the right to amend this Policy from time to time. Any such modifications shall be automatically effective and shall be deemed to have come to the attention of all employees when posted to the RM "SharePoint". RM will endeavour to advise employees of all changes, however, responsibility rests with RM employees to ensure that they are aware of, and fully understand all company policies and procedures.

## 6. REFERENCE DOCUMENTS

Document Name	Hyperlink
CEO-MN_PAIA and POPI Manual	<a href="#">CEO-MN_PAIA and POPI Manual</a>
CEO-POL_Information Security Policy	<a href="#">CEO-POL_Information Security Policy</a>
CEO-POL_Change Management Policy	<a href="#">CEO-POL_Change Management Policy</a>
CEO-PR_Change Management Procedure	<a href="#">CEO-PR_Change Management Procedure</a>
LC-POL_Document Management Policy	<a href="#">LC-POL_Document Management Policy</a>
LC-POL_Communication Policy	<a href="#">LC-POL_Communication Policy</a>
LC_POL_Probity and Licensing Policy	<a href="#">LC_POL_Probity and Licensing Policy</a>
LC-PR_Probity and Licensing Procedure for New Applications	<a href="#">LC-PR_Probity and Licensing Procedure for New Applications</a>
LC-PR_Probity and Licensing Renewals Procedure	<a href="#">LC-PR_Probity and Licensing Renewals Procedure</a>
LC-POL_Related Persons Transaction Policy	<a href="#">LC-POL_Related Persons Transaction Policy</a>
LC-PR_Contract Management Procedure	<a href="#">LC-PR_Contract Management Procedure</a>
LC-POL_LOC Approvals Procedure	<a href="#">LC-POL_LOC Approvals Procedure</a>
LC-POL_Supplier Security Policy	<a href="#">LC-POL_Supplier Security Policy</a>
LC-POL_Document Review Procedure	<a href="#">LC-POL_Document Review Procedure</a>
LC-POL_Identification of Requirements Policy	<a href="#">LC-POL_Identification of Requirements Policy</a>
Appendix 1_List of Legal Regulatory Contractual and Other Requirements	<a href="#">Appendix 1_List of Legal Regulatory Contractual and Other Requirements</a>

LC-POL_Compliance Policy	<a href="#">LC-POL_Compliance Policy</a>
LC-POL_Regulator Liaison Policy	<a href="#">LC-POL_Regulator Liaison Policy</a>
CS-POL_Risk Management Policy	<a href="#">CS-POL_Risk Management Policy</a>
CS-PR_Risk Management Procedure	<a href="#">CS-PR_Risk Management Procedure</a>
CS-POL_Company Vehicles and Garage Card Policy	<a href="#">CS-POL_Company Vehicles and Garage Card Policy</a>
CS-POL_Corporate Social Responsibility Policy	<a href="#">CS-POL_Corporate Social Responsibility Policy</a>
CS-PR_Corporate Social Responsibility Procedure	<a href="#">CS-PR_Corporate Social Responsibility Procedure</a>
CS-POL_Disciplinary Policy	<a href="#">CS-POL_Disciplinary Policy</a>
CS-PR_Disciplinary Procedure	<a href="#">CS-PR_Disciplinary Procedure</a>
CS-POL_Leave Policy	<a href="#">CS-POL_Leave Policy</a>
CS-PR_Leave Procedures	<a href="#">CS-PR_Leave Procedures</a>
CS-POL_Prevent Harassment Policy	<a href="#">CS-POL_Prevent Harassment Policy</a>
CS-PR_Prevent Harassment Procedure	<a href="#">CS-PR_Prevent Harassment Procedure</a>
CS-POL_Recruitment and Employment Policy	<a href="#">CS-POL_Recruitment and Employment Policy</a>
CS-PR_Recruitment and Employment Procedure	<a href="#">CS-PR_Recruitment and Employment Procedure</a>
CS-POL_Termination Policy	<a href="#">CS-POL_Termination Policy</a>
CS-PR_Exit Procedure	<a href="#">CS-PR_Exit Procedure</a>
CS-PR_Company Vehicles Safeguarding Procedure	<a href="#">CS-PR_Company Vehicles Safeguarding Procedure</a>
CS-PR_Poor Work Performance Procedure	<a href="#">CS-PR_Poor Work Performance Procedure</a>
CS-POL_Standard Conditions of Employment Policy	<a href="#">CS-POL_Standard Conditions of Employment Policy</a>
CS-POL_Industrial Relations Policy	<a href="#">CS-POL_Industrial Relations Policy</a>
OP-POL_Helpdesk Policy	<a href="#">OP-POL_Helpdesk Policy</a>
OP-PR_Helpdesk Procedure	<a href="#">OP-PR_Helpdesk Procedure</a>

OP-PR_Measuring Customer Satisfaction Procedure	<a href="#">OP-PR_Measuring Customer Satisfaction Procedure</a>
OP-POL_ Complaints Policy	<a href="#">OP-POL_ Complaints Policy</a>
OP-PR_ Complaints Procedure	<a href="#">OP-PR_ Complaints Procedure</a>
OP-POL_Incident Management Policy	<a href="#">OP-POL Incident Management Policy</a>
OP-PR_Incident Management Procedure	<a href="#">OP-PR Incident Management Procedure</a>
OP-POL_Journal Entry Processing Policy	<a href="#">OP-POL Journal Entry Processing Policy</a>
OP-PR_Journal Entry Processing Procedure	<a href="#">OP-PR Journal Entry Processing Procedure</a>
OP-PR_Hardware Production and Repairs Procedure	<a href="#">OP-PR Hardware Production and Repairs Procedure</a>
OP-POL_Workshop Policy	<a href="#">OP-POL Workshop Policy</a>
OP-PL_Appendix 10_Facilitating the Orders, Assembly And Repairs Of SDLs And PEDs Plan	<a href="#">OP-PL Appendix 10 Facilitating The Orders, Assembly And Repairs Of SDLs And PEDs Plan</a>
FIN-POL_Evaluation of Suppliers Policy	<a href="#">FIN-POL_Evaluation of Suppliers Policy</a>
FIN-PR_Evaluation of Suppliers Procedure	<a href="#">FIN-PR_Evaluation of Suppliers Procedure</a>
FIN-POL_Finance Policy	<a href="#">FIN-POL_Finance Policy</a>
FIN-POL_RM Audit Policy	<a href="#">FIN-POL_RM Audit Policy</a>
FIN-PR_RM Audit Procedure	<a href="#">FIN-PR_RM Audit Procedure</a>
FIN-PR_Invoicing and Collection Procedure	<a href="#">FIN-PR_Invoicing and Collection Procedure</a>
FIN_PR_Payroll Procedure	<a href="#">FIN PR Payroll Procedure</a>
FIN-PR_Procurement Procedure	<a href="#">FIN-PR_Procurement Procedure</a>
FIN-PR_Reconciliation and Submission of Statutory Returns Procedure	<a href="#">FIN-PR Reconciliation and Submission of Statutory Returns Procedure</a>
FIN-PR_Bank Account Processing Procedure	<a href="#">FIN-PR_Bank Account Processing Procedure</a>
FIN-PR_Supplier Complaints Procedure	<a href="#">FIN-PR_Supplier Complaints Procedure</a>
FIN_Appendix_Registry of complaints about Suppliers	<a href="#">FIN Appendix Registry of complaints about Suppliers</a>



TEC-PR_Office 365 and SharePoint User Account Allocation Procedure	<a href="#">TEC-PR_Office 365 and SharePoint User Account Allocation Procedure</a>
TEC-POL_Technical Policy	<a href="#">TEC-POL_Technical Policy</a>
TEC-POL_Logging and Monitoring Policy	<a href="#">TEC-POL_Logging and Monitoring Policy</a>
TEC-PR_Technical Support Procedure	<a href="#">TEC-PR_Technical Support Procedure</a>
OP-POL_Clear Desk and Clear Screen Policy	<a href="#">OP-POL_Clear Desk and Clear Screen Policy</a>
OP-POL_IT Security Policy	<a href="#">OP-POL_IT Security Policy</a>
OP-POL_Information Classification Policy	<a href="#">OP-POL_Information Classification Policy</a>
TEC-PR_New Equipment Procurement Procedure	<a href="#">TEC-PR_New Equipment Procurement Procedure</a>
TEC-PL_Appendix 3_List of Business Continuity Sites	<a href="#">TEC-PL_Appendix 3_List of Business Continuity Sites</a>
TEC-PL_Appendix 5_Key Contacts	<a href="#">TEC-PL_Appendix 5_Key Contacts</a>

**END OF DOCUMENT**

---