1. Introduction

1.1 The Commrisk Group values the importance of protecting the personal information of all its stakeholders and subscribes to the principles outlined in the ***Protection of Personal Information Act, No. 4 of 2013 (*POPIA)** and all other related and/or subordinate legislation.

1.2 Commrisk is committed to safeguarding the personal information that it collects, stores and processes in a responsible and lawful manner that places value on everyone's right to privacy.

2. Purpose

2.1 The purpose of this policy is to:

- 2.1.1 promote the protection of personal information processed by the Commrisk Group entities and their service providers.
- 2.1.2 uphold transparency regarding the information that we collect, what we use it for, how we use it and who we share it with.
- 2.1.3 enable the effective monitoring of compliance per the POPIA requirements.
- 2.1.4 enable Commrisk to conduct POPIA impact assessments and implement corrective action for identified shortfalls.
- 2.1.5 create and maintain awareness of POPIA through regular interactive communication with employees, service providers and any other interested parties.

3. Scope

3.1 This policy applies to the following Commrisk Group entities and their staff (full time employees, directors and independent representatives/agents):

- 3.1.1 Commrisk Insurance Brokers (Pty) Ltd
- 3.1.2 Commrisk Insurance Brokers Welkom (Pty) Ltd
- 3.1.3 Commrisk Eastern Cape (Pty) Ltd
- 3.1.4 Multi Admin (Pty) Ltd
- 3.1.5 Multi Risk Investment Holdings (Pty) Ltd

3.2 Any reference to *"Commrisk"* or *"Commrisk Group"* or *"company"* in this document shall be taken to mean the above entities collectively.

4. Key Definitions

4.1 **Consent** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

4.2 **Data subject** means the person to whom personal information relates.

4.3 **Operator** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

4.4 **Personal information** means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, but not limited to;

4.4.1 information relating to 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;
4.4.2 information relating to the education or the medical, financial, criminal or employment history of the person;
4.4.3 any identifying number, symbol, email address, physical address, telephone number, location information, inline identifier or other particular assignment to the person.
4.4.4 the biometric information of the person.
4.4.5 the personal opinions, views or preferences of the person;
4.4.6 correspondence sent by the person that is implicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
4.4.7 the views or opinions of another individual about the person; and
4.4.8 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.

4.5 **Processing** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including;

4.5.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
4.5.2 dissemination by means of transmission, distribution or making available in any other form; or
4.5.3 merging, linking, restriction, degradation, erasure or destruction of information

4.6 **Information Regulator** means the Regulator as established in terms of section 39 of the *Protection of Personal Information Act 4 of 2013*.

4.7 **Responsible party** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

5. Personal Information held by Commrisk

5.1 Commrisk collects, processes, stores and may share personal information from the following data subjects:

5.1.1 Customers and/or their authorised representatives
5.1.2 Employees, directors and independent representatives/agents
5.1.3 Third party service providers
5.1.4 Commrisk website users

5.2 The type and amount of personal information collected, processed, stored and/or shared with relevant third parties by Commrisk is strictly dependent on the purpose for which it is required, which could be:

5.2.1 to provide financial and intermediary services to potential and existing customers;
5.2.2 for recruitment and employment purposes;
5.2.3 to fulfil contractual obligations;
5.2.4 for marketing research and statistical purposes;
5.2.5 to comply with legislative and regulatory requirements;
5.2.6 to detect and prevent unlawful activity under relevant applicable legislation;
5.2.7 for other lawful reasons not covered by the above.

6. Processes and Procedures

6.1 Collection of Information

6.1.1 Commrisk only collects personal information from data subjects from whom consent has been obtained.
6.1.2 Where personal information is obtained from third parties, Commrisk requires the third party to be in possession of consent for the collection and sharing of the information.
6.1.3 Personal information may only be collected, processed and stored for specific and lawful purposes disclosed to the data subjects.
6.1.4 Where purposes contemplated in clause 6.1.3 above, Commrisk will advise data subjects of the change and seek consent for use of the information for the new purpose/s.

6.2 Storage, Processing and Protection of Information

6.2.1 Commrisk stores, processes and shares personal information to the extent required for the purpose for which the personal information has been obtained.
6.2.2 From time to time, Commrisk checks the accuracy, completeness and relevance of the personal information it holds.
6.2.3 Personal information is stored electronically and in hard copy format.
6.2.4 Access to such information is controlled and restricted by physical and virtual security controls and only granted to employees or third parties with requisite authorisation and a legitimate need to access such information, for the disclosed purpose per clause 5.2.
6.2.5 Access to stored personal information is continuously monitored and may be limited or revoked as may be deemed necessary in line with legislation and the company's information technology and other relevant policies.

6.3 Retention and Deletion of Information

6.3.1 Commrisk will retain personal information on its systems and in its archives for as long as is permitted under POPIA, PAIA and other legislation for legal and legitimate purposes.

6.3.2 Where consent is been revoked by a data subject or personal information is no longer needed, such personal information is deleted or anonymised beyond forensic reconstruction.

6.4 Information Security and Other Protocols

6.4.1 All Commrisk employees are bound by this and other relevant company policies covering information security.

6.4.2 On termination of employment, access to Commrisk systems and files is immediately withdrawn for the employee leaving the company per the line manager's instructions.

6.4.3 Terminated employees remain bound by a restraint preventing them from using personal and other information held by Commrisk and are required to confirm that they do not possess any personal information at the time of leaving employment.

6.4.4 Failure to adhere to clause 6.4.3 above may lead to, but is not limited to;

6.4.4.1 enforcement of the restraint order through legal action, if necessary.

6.4.4.2 reporting of the terminated employee to the Information Regulator.

6.4.5 Internal and external communication is filtered through the secure Office365 environment.

6.4.6 Virtual information security protocols are periodically checked and reviewed to prevent, detect and mitigate the risk of loss, unlawful access and unauthorised disclosure of personal information.

6.4.7 Physical access to areas in which hard copy files with sensitive personal information are kept or servers are located is controlled and restricted.

6.4.8 Obsolete hardware and hard copy files containing personal information are wiped or destroyed beyond forensic reconstruction or discarded to POPIA compliant recycling and document destruction service providers.

6.5 Information System Breaches

6.5.1 In the event of a system breach which may compromise the confidentiality, integrity and/or availability of personal information, Commrisk will immediately implement the following measures:

6.5.1.1 Notify all affected data subjects, insurer partners and other affected persons directly via the policy admin system bulk email facility and/or the Outlook email client the nature of the breach, potential consequences to the data subjects and remedial action being taken by Commrisk.

6.5.1.2 If the identities of the affected data subjects cannot be established, a notification with the information in clause 6.5.1.1 above will be displayed on the Commrisk website.

6.5.1.3 Once the nature, extent and reason for the breach has been determined, remedial action to rectify the breach and prevent future breaches will be implemented.

6.5.1.4 Continue to provide updated information as it becomes available and any remedial action to data subjects, insurer partners and other affected persons per 6.5.1.1 and 6.5.1.2 above.

7. Roles and Responsibilities

7.1 In line with the provisions of the *Protection of Personal Information Act* (POPIA) and the *Promotion of Access to Information Act* (PAIA), Commrisk has an **Information Officer** who is responsible for;

7.1.1 developing and maintaining policies and procedures in line with POPIA.
7.1.2 conducting the POPIA impact assessment and ensuring that corrective action is put in place for identified shortfalls.
7.1.3 ensuring ongoing employee awareness of the requirements of POPIA and PAIA.
7.1.4 attending to data subject requests and complaints made in terms of POPIA and PAIA.
7.1.5 on-going monitoring of compliance with POPIA and PAIA, including the PAIA Manual.
7.1.6 processing requests for information or access to information in terms of POPIA, PAIA and the Commrisk PAIA Manual.

7.2 Details of Commrisk's Information Officer are as follows:

Information Officer	Peter Gerard van Niekerk
Telephone number	011 840 7000
Email address	info@commrisk.co.za
Physical address	Block A – Fourways View Office Park Corner 1210 Sunset Boulevard & Sunrise Avenue Lonehill Ext 44, Johannesburg, 2191
Postal address	P O Box 254 Pinegowrie 2123

8. Complaints and objections

8.1 Per the provisions of POPIA, all data subjects have the right to:

8.1.1 request Commrisk to confirm, free of charge, whether or not Commrisk holds their personal information *(refer to the Commrisk PAIA manual)*.
8.1.2 request Commrisk to provide a description of the personal information it holds about them, and to explain why and how that information is being processed *(refer to the Commrisk PAIA manual).*
8.1.3 request Commrisk to consider their objections to the processing of their personal information *(complete Form 1 – Annexure B).*
8.1.4 request Commrisk to correct or amend and reflect the true nature or form of their personal information *(complete Form 2 – Annexure C).*
8.1.5 Lodge a complaint with the Information Regulator *(complete Form 5 – Annexure D)*

8.2 Data subjects who wish to exercise their rights per clauses 8.1.1 to 8.1.4 can contact the Commrisk Group's Information Officer using the details in given in clause 7.2.

8.3 Should the data subject not be satisfied with the outcome or response to their request, or lack thereof, from the Information Officer, they can then lodge a complaint with the **Information Regulator** per clause 8.1.5 above using the contact details below:

Telephone	010 023 5200
Email address	POPIAComplaints@inforegulator.org.za
Website	https://inforegulator.org.za/
Physical address	JD House 27 Stiemens Street Braamfontein Johannesburg 2001
Postal address	P O Box 31533 Braamfontein Johannesburg 2017

9. Related Policies

9.1 This policy should be read in conjunction with the Commrisk Group's:

9.1.1 Promotion of Access to Information Act (PAIA) Manual
9.1.2 P&P 08 - Business Code of Conduct
9.1.3 P&P 26 - Electronic Communications Policy
9.1.4 P&P 36 - Information Security Policy
9.1.5 P&P 43 - Data Back-up and Recovery Policy

10. Document Control Summary

Document	Version 2023_10
Updated by	Lewis Chiripanyanga
Approved by	Peter Gerard van Niekerk Director – Commrisk Insurance Brokers (Pty) Ltd Director – Commrisk Insurance Brokers Welkom (Pty) Ltd Director – Commrisk Eastern Cape (Pty) Ltd Director – Multi Admin (Pty) Ltd Director – Multi Risk Investment Holdings (Pty) Ltd
Approved date	11 October 2023
Effective date	01 November 2023
Next review date	April 2024

Annexure A

POPIA Employee Commitment Form

The Employee Commitment below must be signed off by all new employees during their induction into the company:

I understand and acknowledge that my duties may include the processing of the personal information of clients. Such processing shall be done under the authorisation of the Responsible Party which is Commrisk Insurance Brokers (Pty) Ltd and any of its subsidiaries and associated companies/entities. (Referred to in this clause as "Commrisk")

You agree to be bound by and to process information according to the requirements of the Protection of Personal Information Act, the Promotion of Access to Information Act, the Commrisk internal policy on Protection of Personal Information, the Promotion of Access to Information (PAIA) manual and any other applicable legislation (copies of these Acts and policies can be obtained from Human Resources).

Such processing requirements shall include, but not be limited to the following:

1. You will ensure that the Responsible Party (Commrisk), has the required authority to collect and process client information being processed by yourself.

2. All client information shall be treated as confidential and under no circumstances will you pass on such information to any third party without written consent from the client. (This will normally be on the proposal form and the *"Consent to Information Sharing"* contained in the policy schedule.)

3. You will, at all times, adhere to company data and information security policies and procedures and other relevant security measures (e.g., passwords and system access codes).

4. It will be a disciplinary offence to provide any other person, whether an employee or not, with your password and/or access code without written permission from your manager.

5. Should you be aware of any data security breach, or that a client's personal information has been sent to any third party without that client's written permission, you will report this to your manager as soon as you become aware of the incident.

6. On termination of employment, you agree that you will not retain any information covered by POPIA and that you will delete all such information from any of your personal devices such as cell phones and laptops/tablets.

I _____ understand and agree to abide by the above requirements.

_____ _____

SIGNATURE: **DATE:**

Annexure B (Form 1)

Objection to the Processing of Personal Information in terms of Section 11 (3) of the Protection of Personal Information Act, 2013 (Act 4 of 2013)

Regulations Relating to the Protection of Personal Information 2018
[Regulation 2]

Notes:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Full registered name of data subject	
Reg/ID/Passport no.	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	
B	**DETAILS OF RESPONSIBLE PARTY**
Full registered name of responsible party	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at _____ on this _____ day of _____ 20___

_____

SIGNATURE OF DATA SUBJECT/DESIGNATED PERSON:

Annexure C – (Form 2)

Request for Correction or Deletion of Personal Information or Destroying or Deletion of a Record of Personal Information in terms of Section 24 (1) of the Protection of Personal Information Act, 2013 (Act 4 of 2013)

Regulations Relating to the Protection of Personal Information 2018
[Regulation 3]

Notes:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this form and sign each page.*
3. *Complete as is applicable.*

Request for *(mark the appropriate box with an "X"):*

☐ Correction or deletion of the personal information about the data subject which is in possession or control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or control of the responsible party.

A	**DETAILS OF DATA SUBJECT**
Full registered name of data subject	
Reg/ID/Passport no.	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	
B	**DETAILS OF RESPONSIBLE PARTY**
Full registered name of responsible party	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	

C	INFORMATION TO BE CORRECTED/DELETED/DESTROYED
D	**REASONS FOR CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1)(a) WHICH IS IN POSSESSION OR CONTROL THE RESPONSIBLE PARTY; and or** **REASONS FOR DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1)(b) WHICH IS IN POSSESSION OR CONTROL THE RESPONSIBLE PARTY** *(Please provide detailed reasons for the request)*

Signed at _____ on this _____ day of _____ 20___

_____

SIGNATURE OF DATA SUBJECT/DESIGNATED PERSON:

Annexure D – (Form 5)

Complaint Regarding Interference with the Protection of Personal Information / Complaint Regarding Determination of an Adjudicator in terms of Section 74 of the Protection of Personal Information Act, 2013 (Act 4 of 2013)

Regulations Relating to the Protection of Personal Information 2018
[Regulation 7]

Notes:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this form and sign each page.*
3. *Complete as is applicable.*

Complaint regarding *(mark the appropriate box with an "X"):*

☐ Alleged interference with the protection of personal information.

☐ Determination of an Adjudicator.

PART I	**ALLEGED INTEREFERENCE WITH THE PROTECTION OF PERSONAL INFORMATION IN TERMS OF SECTION 74 (1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT No. 4 of 2013)**
A	**PARTICULARS OF COMPLAINANT**
Full registered name of data subject	
Reg/ID/Passport no.	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	
B	**PARTICULARS OF RESPONSIBLE PARTY INTEREFERING WITH PROTECTION OF PERSONAL INFORMATION**
Full registered name of responsible party	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	

C	REASONS FOR COMPLAINT *(Please provide detailed reasons for the complaint)*

PART II	COMPLAINT REGARDING DETERMINATION OF ADJUDICATOR IN TERMS OF SECTION 74 (2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT No. 4 of 2013)
A	**PARTICULARS OF COMPLAINANT**
Full registered name of data subject	
Reg/ID/Passport no.	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	
B	**PARTICULARS OF ADJUDICATOR AND RESPONSIBLE PARTY**
Full registered name of responsible party	
Residential, postal or business address	
	Code ( )
Contact number/s	
Contact email address	

C	**REASONS FOR COMPLAINT** *(Please provide detailed reasons for the complaint)*

Signed at _____ on this _____ day of _____ 20___

_____

SIGNATURE OF DATA SUBJECT/DESIGNATED PERSON: