SafetySA®

Making the World a Safer Place

AssureCLOUD

Member of CTi Group

SafetyCLOUD

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000

(as amended)

Our Purpose

To make the world a safer place

Our Principles

Care

We **care intensely** about providing **excellent service** to our customers, about making the world a **safer place**, about **working well together**

Courage

To say what you think even if it's uncomfortable, to **try new things**, to **push boundaries**, to **make the decision**, to **question**, to **take a smart risk**, to **fail and fail fast**

Passion

We bring energy to all we do – always **giving our best – being the best** at what we do, **not settling for average**, going the **extra mile**

Innovation

We **thrive on change** and are not limited by how things have always been done. We **create solutions** which **solve hard problems, reduce complexity**, provide **new insights** and **improve safety**

Accountability

We **get the job done** and **take ownership** for **solving problems** that arise **on our watch**

In accordance with the provisions of the Protection of Personal Information Act No. 4 of 2013 ("POPIA") Safety SA Group has implemented the necessary POPIA policies and procedures to ensure full compliance with POPIA. Please refer to the Safety SA's privacy notice (https://safetysa.com/privacy-notice/)

Contents

1. Safety SA Group 4
2. Safety SA Group Privacy Notices 4
3. Acronyms and Abbreviations 4
4. References 4
5. Purpose of the Manual 5
6. Key Contact Details for Access to Information of the Safety SA Group 6
7. Contact Information for the Information Regulator of South Africa 7
8. Guide on How to use PAIA and How to Obtain Access to the Guide 7
9. Request for Records 8
10. Granting of Request for Information 8
11. Denial of Request for Information 8
12. Fees 9
13. Request for Records Containing Third Party Information 9
14. Records that cannot be found or do not exist 10
15. Records of Safety SA Group Which are Available in Accordance with any Other Legislation 10
16. Why do we Collect and Process Personal Information? 10
17. Exercising POPIA Rights 13
18. Types of Personal Information We Collect and Process 13
19. Transborder – Flow of Information 14
20. Security Measures 14
21. Exercising Data Subject Rights under POPIA 14
22. Marketing and Communication 15
23. Availability of the Manual 15

1. Safety SA Group

1.1. Safety SA Holdco (Pty) Ltd ("herein referred to as Safety SA Group") is a registered legal entity established within the laws of South Africa with CIPC Registration Number: 2017/254215/07. The PAIA Manual is relevant and has application for the major subsidiaries of Safety SA Group as set out in the list below.

1.2. In this PAIA Manual, any reference to Safety SA Group includes any of the entities and / or brand names as listed below:

- Safety SA Holdco (Pty) Ltd, registration number 2017/254215/07 ("Safety SA Holdco");
- Safety SA Solutions (Pty) Ltd, registration number 1980/003286/07 ("Safety SA Solutions").

SafetyCloud, brand name, the legal entities listed below forms part of the SafetyCloud brand;

- NOSA (Pty) Ltd, registration number 2003/029513/07 ("NOSA");
- NOSA Logistics (Pty) Ltd, registration number 2003/010541/07 ("NOSA Logistics");
- National Quality Assurance (Pty) Ltd, registration number 2001/023856/07 ("NQA");
- NOSA Auditing and Inspection Services (Pty) Ltd, registration number 2005/013629/07 ("NAIS").

AssureCloud, brand name, the legal entities listed below forms part of the AssureCloud brand

- Aspirata Auditing Testing and Inspection (Pty) Ltd, registration 2013/00208/07 ("Aspirata");
- World of Ethics (Pty) Ltd, registration number 2019/461436/07 ("WOE");
- Ethical Excellence (Pty) Ltd, registration number 2019/405347/07 ("Ethical Excellence");
- Ethikos Academy (Pty) Ltd, registration number 2020/143585/07 ("Ethikos Academy"); and
- Quality and Safety Risk Professional Services International (Pty) Ltd, registration number 2002/016110/07 ("QPRO").

2. Safety SA Group Privacy Notices

Safety SA Holdco	https://safetysa.com/privacy-notice/
AssureCloud	https://assurecloud.co.za/privacy-notice/
SafetyCloud	https://safetycloud.co.za/privacy-policy/

3. Acronyms and Abbreviations

3.1.	"CEO"	Chief Executive Officer
3.2.	"DIO"	Deputy Information Officer
3.3.	"IO"	Information Officer
3.4.	"Minister"	Minister of Justice and Correctional Services
3.5.	"PAIA"	Promotion of Access to Information Act No. 2 of 2000(as amended)
3.6.	"POPIA"	Protection of Personal Information Act No. 4 of 2013
3.7.	"Regulator"	Information Regulator
3.8.	"Republic"	Republic of South Africa

4. References

4.1. Section 17(1) of PAIA- For the purposes of PAIA, each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as deputy information officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.

4.2. Section 56(a) of POPIA- Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.

4.3. Section 11(1) of PAIA- A requester must be given access to a record of a public body if that requester complies with all the procedural requirements in PAIA relating to a request for access to that record; and access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

4.4. Section 50(1) of PAIA- A requester must be given access to any record of a private body if-

4.4.1. that record is required for the exercise or protection of any rights;

4.4.2. that person complies with the procedural requirements in PAIA relating to a request for access to that record; and

4.4.3. access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

4.5. Section 14(1) of PAIA- The information officer of a public body must, in at least three official languages, make available a manual containing information listed in paragraph 4 above.

4.6. Section 51(1) of PAIA- The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.

4.7. Section 15(1) of PAIA- The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access

4.8. Section 52(1) of PAIA- The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access

4.9. Section 22(1) of PAIA- The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

4.10. Section 54(1) of PAIA- The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

4.11. Section 92(1) of PAIA provides that – "The Minister may, by notice in the Gazette, make regulations regarding-

4.11.1. any matter which is required or permitted by this Act to be prescribed;

4.11.2. any matter relating to the fees contemplated in sections 22 and 54;

4.11.3. any notice required by this Act;

4.11.4. uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and

4.11.5. any administrative or procedural matter necessary to give effect to the provisions of this Act."

5. Purpose of the Manual

This PAIA Manual is useful for the public to-

5.1. check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

5.2. have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

5.3. know the description of the records of the body which are available in accordance with any other legislation;

5.4. access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

5.5. know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

5.6. know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

5.7. know the description of the categories of data subjects and of the information or categories of information relating thereto;

5.8. know the recipients or categories of recipients to whom the personal information may be supplied;

5.9. know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

5.10. know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

6. Key Contact Details for Access to Information of the Safety SA Group

6.1. **Information Officer (CEO) for the Safety SA Group**

Designation	Name	Contact Number	Email Address
Information Officer	Jeffrey Zeng	+27872868222	compliance@safetysa.com

6.2. **Deputy Information Officer for the Safety SA Group**

Designation	Name	Contact Number	Email Address
Deputy Information Officer	Desire Jordaan	+27872868222	desire.jordaan@safetysa.com
Deputy Information Officer	Martin Joubert	+27872868222	martin.joubert@safetysa.com
Deputy Information Officer	Miles Du Plessis	+27872868222	Miles.duplessis@safetysa.com

6.3. **Access to information general contacts**

6.3.1. Email: compliance@safetysa.com

6.3.2. SMS or WhatsApp: +27 67 596 7993

6.3.3. Ordinary Business Hours:
Monday to Friday
08h00 – 17h00
Excluding Public Holidays

6.4. **Safety SA Group Head Office**

Attention	**Deputy Information Officer**
Physical Address	Porta Nova Building, Gazelle Close, Corporate Park South, Old Pretoria Road, Randjesfontein, Midrand, 1683
Postal Address	Porta Nova Building, Gazelle Close, Corporate Park South, Old Pretoria Road, Randjesfontein, Midrand, 1683
Telephone Number	+27872868222

E-mail	compliance@safetysa.com
Safety SA Holdco	https://safetysa.com/
AssureCloud	https://assurecloud.co.za/
SafetyCloud	https://safetycloud.co.za/
NQA	https://www.nqa.com/en-za

7. Contact Information for the Information Regulator of South Africa

7.1. Data subjects have the right to lodge a complaint to the Information Regulator of South Africa.

Attention	**Information Regulator of South Africa**
Physical Address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg
Postal Address	P.O Box 31533, Braamfontein, Johannesburg, 2017
Telephone Number	010 023 5200
E-mail	enquiries@inforegulator.org.za
Website	https://eservices.inforegulator.org.za/

7.2. Prescribed POPIA forms relating to requests for access, correction, deletion and objections to processing may be obtained from the Information Regulator or from the Information Officer upon request.

8. Guide on How to use PAIA and How to Obtain Access to the Guide

8.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

8.2. The Guide is available in each of the official languages and in braille.

8.3. The aforesaid Guide contains the description of-

8.3.1. the objects of PAIA and POPIA;

8.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of-

8.3.2.1. the Information Officer of every public body, and

8.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA;

8.3.3. the manner and form of a request for-

8.3.3.1. access to a record of a public body contemplated in section 11; and

8.3.3.2. access to a record of a private body contemplated in section 50;

8.3.4. the assistance available from the IO of a public body in terms of PAIA and POPIA;

8.3.5. the assistance available from the Regulator in terms of PAIA and POPIA;

8.3.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging.

8.3.6.1. an internal appeal;

8.3.6.2. a complaint to the Regulator; and

8.3.6.3. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

8.3.7. the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

8.3.8. the provisions of sections 15[7] and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

8.3.9. the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and

8.3.10. the regulations made in terms of section 92.

8.4. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

8.5. The Guide can also be obtained-

8.5.1. upon request to the Information Officer;

8.5.2. from the website of the Regulator (PAIA Guidelines - Information Regulator (inforegulator.org.za))

8.6. A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours-

8.6.1. English - PAIA Guide - English_Upd 5 Sept (inforegulator.org.za)

8.6.2. isiZulu - PAIA Guide - isiZulu_Upd 21 Sept (inforegulator.org.za)

9. Request for Records

9.1. Requests for records or Personal Information may be submitted by hand delivery, registered post, email, SMS, WhatsApp, telephonically, or through any other reasonable communication channel made available by Safety SA Group.

9.2. Requests for records must be directed to the Information Officer who shall consider the request and provide a decision within 30 (thirty) days of having received the request or having received the prescribed particulars in terms of section 53(2) of PAIA.

9.3. A request for information may be refused by the Safety SA Group if it does not comply with PAIA or if the Safety SA Group believes that there is a valid ground for objection in terms of PAIA.

9.4. The person requesting the information must provide the Safety SA Group with sufficient information for the Information Officer to identify the record and the person requesting the record.

9.5. The person requesting information must indicate the type of access required and his/her contact details including e-mail address, and postal address.

9.6. Should the requesting person prefer a certain means of communication, such means of communication must be included in the request for information.

9.7. Should a request for records be made on behalf of a third party, authority to do so must be provided to the Information Officer.

9.8. Telephonic requests shall be documented by Safety SA Group and retained as part of the official request record.

9.9. Safety SA Group may require written confirmation of a telephonic request to verify the identity of the requester and ensure accurate processing.

10. Granting of Request for Information

10.1. Should a request be granted, the Safety SA Group shall provide the requesting person with the following information:

10.2. the access fee payable by the requesting person;

10.3. the type of access which will be granted; and

10.4. notice that the requesting person may approach a competent court to dispute the access fee or the type of access to be granted.

10.5. Once a request has been granted, the records shall be made available to the requesting person once the relevant fee has been paid.

11. Denial of Request for Information

11.1. A request for access to information may be refused in the following circumstances:

11.2. protecting Personal Information that the Safety SA Group holds regarding a third party from unreasonable disclosure;

11.3. protecting commercial information that the Safety SA Group holds regarding a third party which may harm the commercial or financial interests of such third party;

11.4. if the disclosure would result in a breach of a duty of confidence owed to a third party;

11.5. if the disclosure would jeopardise the safety or life of natural person;

11.6. if disclosure would prejudice or impair the security of property or means of transport of a person;

11.7. if disclosure would prejudice or impair the protection of a person who is subject to a witness protection scheme;

11.8. if disclosure would prejudice or impair the protection of the safety of the public;

11.9. the record is privileged from production in legal proceedings unless privilege in relation to such record has been waived;

11.10. if the record is a computer programme;

11.11. disclosure of the record will put the Safety SA Group at a disadvantage in contractual or other negotiations or prejudice the Safety SA Group in commercial competition;

11.12. disclosure of the record would harm the commercial or financial interests of the Safety SA Group; and

11.13. records containing information about research being carried out or about to be carried out on behalf of a third party or a company which is related to the Safety SA Group, and which have not been made public by the Safety SA Group.

11.14. Should a request be refused, the Safety SA Group shall provide the requesting person with the following information –

11.14.1. adequate reasons for the refusal including the relevant sections of PAIA; and

11.14.2. notice that the requesting person may lodge an application with a competent court against the refusal and against the procedure including the period for lodging the application.

12. Fees

12.1. A non-refundable request fee is payable to the Safety SA Group upon the submission of the request.

12.2. A requesting party who has made a request for access to records and such request has been granted must pay an access fee to the Safety SA Group for the search and preparation of the records and any time reasonably required which exceeds the prescribed hours for searching and preparation arrangements.

12.3. The prescribed forms and fees are available on the website of the Department of Justice and Constitutional Development.

13. Request for Records Containing Third Party Information

13.1. Should records be requested that contain information pertaining to a third party, the

13.2. Group is obliged to attempt to contact the third party to inform it of the request and to provide it with the opportunity to respond to the request by consenting or providing reasons why the access should be refused.

13.3. Should the third party provide reasons for the support of or against providing access, the Information Officer will consider such reasons in determining whether access should be granted.

13.4. The requesting party may appeal the decision of the Information Officer to a competent court in the Republic of South Africa in accordance with PAIA.

14. Records that cannot be found or do not exist

14.1. Should all reasonable steps be taken by the Safety SA Group to find a requested record and there are reasonable grounds to believe that the record:

14.2. is in the Safety SA Group's possession but cannot be found; or

14.3. does not exist,

14.4. then the Information Officer shall notify the requesting party that it is not possible to provide the requesting party access to such record.

15. Records of Safety SA Group Which are Available in Accordance with any Other Legislation

15.1. The Safety SA Group is required to hold records in terms of the following Acts:

15.1.1. Basic Conditions of Employment Act, No. 75 of 1997;

15.1.2. Companies Act, No. 71 of 2008;

15.1.3. Compensation for Occupational Injuries and Diseases Act No. 130 of 1993;

15.1.4. Consumer Protection Act No. 68 of 2008;

15.1.5. Currency and Exchanges Act No. 9 of 1933;

15.1.6. Electronic Communications and Transactions Act No. 25 of 2002;

15.1.7. Employment Equity Act No. 55 of 1998;

15.1.8. Financial Intelligence Centre Act No. 38 of 2001;

15.1.9. Income Tax Act, No. 58 of 1962;

15.1.10. Labour Relations Act No. 66 of 1995;

15.1.11. National Credit Act No. 34 of 2005;

15.1.12. Occupational Health and Safety Act No. 85 of 1993;

15.1.13. Regulation of Interception of Communications Act, No. 70 of 2002;

15.1.14. Skills Development Act No. 97 of 1998;

15.1.15. Skills Development Levies Act No. 9 of 1999;

15.1.16. Trade Marks Act No. 194 of 1993;

15.1.17. Unemployment Insurance Act No. 63 of 2001;

15.1.18. Unemployment Insurance Contributions Act No. 4 of 2002; and

15.1.19. Value Added Tax Act No. 89 of 1991.

16. Why do we Collect and Process Personal Information?

16.1. Our reason for collecting your personal information depends on the activity at hand. Our intention for collecting personal information, including but not limited to:

16.1.1. Contests, Email Newsletters and Inquiry Information to allow us to be in contact with you in relation to your inquiry or your participation in Safety SA's email newsletters or the contests, to personalise our services for you, notify you of special offers or promotions that we believe may be of interest to you and send our newsletters or to provide you with customer service, and to monitor our provision of customer service. In some cases, we may use some of your Personal Data for external communications purposes, for example, by making a press release about a contest winner.

16.1.2. Website Information to monitor and administer the contests you may enter and your inquiries, to analyse trends, usage and activities with users on our website, to ensure its technological compatibility, to help us create websites that best suit our users' interests and preferences and to help identify products and services, site features, advertisements, and offers that may be of particular interest to you (for example, as part of an extended market research). We also use

website information to monitor and control the security of our website and prevent cyber security incidents, as well as to collect feedback on the website usage, provide IT support to online visitors and gauge success of our marketing initiatives.

16.1.3. Portal Subscriber Information to administer the specific relationship, fulfil contractual obligations, deal with quality issues, assist with business planning and development, assist suppliers or other portal subscribers to achieve goals, and administer incentive programmes. In certain limited cases, we also use Personal Data to facilitate billing and invoicing or for the purpose of product traceability or compliance with regulatory requirements or contractual requirements.

16.1.4. Passwords and Password Aide-memoire Questions and Answers to register yourself online in a secure way and help you register if you forget your password. We request that you choose a password that is unique to every account and that you do not use sensitive information or financial information as an aide-memoire (for example, your bank account credentials).

16.1.5. CCTV Footage to maintain a safe and secure environment for our people, visitors, products, services, and processes; where applicable.

16.1.6. Information Collected on Social Media Accounts to contact you via your social media accounts, to answer your inquiries and better engage with our customers.

16.1.7. Research & Development and Market Research Information to perform market research, improve our products and services, for R&D purposes, and for the study and understanding of the business and preferences of consumers or operators.

16.1.8. Visitor Information to comply with building safety obligations, to identify the people that are entering our premises and for health reasons.

16.1.9. Photos and Videos and Related Content to communicate about our events, meetings, conferences, products, partnerships and other relationships, on our websites, via our social media accounts, via press releases, and other corporate communications and marketing materials. In some cases, we may ask you to provide us with your email address to send you the pictures and videos, we may collect your professional details to contact you back about our products and services, or, if you are a government official, we may collect and use data revealing your political opinions, to facilitate corporate communications, corporate affairs, recruitment and engagement of individuals, and for public affairs purposes.

16.1.10. CV/Resumes and Relevant Information for Recruitment to enable us to recruit the right people.

16.1.11. Information relating to Sourcing and Procurement to set up the contractual terms with our suppliers, to pay for our suppliers' products or services, to perform recalls and to call warranties, to comply with accounting obligations applicable to us, to conduct demand planning and generally to facilitate the relationship with our suppliers.

16.1.12. Information relating to Individual Consumers of our products and services to, if and to the extent permitted by applicable law, provide individual consumers of our products and services with marketing communications promoting our products and services (or those of third parties), to better understand our consumers' needs, to address complaints on our products and services, and more generally to improve our relationships with individual consumers.

16.1.13. User-generated Content received through our Online Presence to better engage with our customers or individual consumers of our products, to interact with our customers, and to address complaints.

16.1.14. Information about Inventors to apply for or assign patents or similar registered intellectual property rights for the benefit of Safety SA.

16.1.15. Information to Protect against Serious Threats to Health to allow us to protect you and other individuals, such as customers or contractors, and to help contain the threat in the public interest.

16.1.16. ID and Passport Information to help us prevent unauthorised individuals from accessing, changing or deleting your Personal Data.

16.1.17. Internal Administrative Purposes to allow us to administer the business, including for purposes of audit, data analysis, sustainable cost advantage, compliance, governance and legal, corporate social responsibility (CSR), security, accounts payable and receivable validation, and database records.

16.1.18. Combined Information, if and to the extent permitted by applicable law, to better understand your needs and interests. We may combine the Personal Data that you have provided to us with other information we have collected about you, whether online or offline, or with data obtained from other sources (such as our third-party advertising partners). This way we can provide you with the most optimal customer experience and serve you advertisements or otherwise interact with you in ways that are specifically tailored to your interests and preferences. For example, if and to the extent permitted by applicable law: we may share a cryptographic hash of your email address with a third-party advertising partner, such as social networking sites where you are a registered user (by using the hashing process, your email address is not disclosed to the third party). If the hashed email address from us matches a hashed email address that the third party advertising partner has, the third party identifies you as part of a group of individuals to whom our ads might be served on its website or on other media; and a third party advertising partner may provide us with certain aggregate demographic information about the demographic group to which you belong, which is obtained from your profile and materials with the third party advertising partner.

16.1.19. De-identified/Anonymised Information to identify trends, manage our business, develop statistical information, understand how we are performing, or develop relevant products, services or offers derived from combining Personal Data with other information, as explained above.

16.2. Depending on the circumstances, we may also use your Personal Data for the following purposes:

16.2.1. For corporate communications purposes and for public affairs purposes (including, if necessary, to issue a public response to specific complaints)

16.2.2. To respond to your comments and questions (problem resolution)

16.2.3. To provide customer service (for example, product recalls, tracking, and responding to product quality concerns)

16.2.4. To conduct sales and market research (for example, through surveys)

16.2.5. To conduct research and development (for example, through product concept correspondence)

16.2.6. To register yourself when we organise events

16.2.7. If and to the extent permitted by applicable law, for direct marketing purposes

16.2.8. To improve business relations

16.2.9. For public affairs purposes

16.2.10. To protect against and prevent fraud, or other criminal activities, unauthorized transactions, claims and other liabilities, and to manage risk exposure

16.2.11. To handle legal disputes

16.2.12. To conduct corporate transactions (including mergers, acquisitions, and divestments); and

16.2.13. To improve and enhance our products and services, in general.

16.3. We will not use Personal Data for any purposes that are incompatible with those outlined in this Policy, unless you give us your free and informed consent for additional specific purposes.

17. Exercising POPIA Rights

17.1. In addition to the rights of access to records provided under PAIA, Data Subjects are entitled to exercise their rights under the Protection of Personal Information Act, 4 of 2013 ("POPIA"), including the right to:

17.1.1. Access personal information held by Safety SA Group;

17.1.2. Request correction, updating, deletion or destruction of personal information where permitted by law;

17.1.3. Object to the processing of personal information;

17.1.4. Withdraw consent previously provided; and

17.1.5. Lodge a complaint with the Information Regulator.

17.2. The procedures, submission channels, response timeframes, identity verification requirements, objection processes and prescribed POPIA forms applicable to the exercise of these rights are contained in the Safety SA Group Privacy Notice.

17.3. The Privacy Notice is available:

17.3.1. On the Safety SA Group website;

17.3.2. Upon request from the Information Officer or Deputy Information Officers; and

17.3.3. By emailing compliance@safetysa.com.

17.3.4. Requests may be submitted through reasonably accessible channels including email, hand delivery, post, telephone, SMS and WhatsApp as set out in the Privacy Notice.

18. Types of Personal Information We Collect and Process

GENERAL PERSONAL INFORMATION – Individual			
Full Name/s and Surname	Identification / Passport Details / Date of birth / Age	Contact Details – email / telephonic	Gender, Race or Ethnic Origin
Qualifications / Registrations / Memberships / Accreditations	Employment History / Salary Information	Complaints and Disciplinary Records	Personal Tax Income Reference
Financial Information / Banking Details	Union Affiliations	Contactable References	Driver's License
Physical / Mental / Medical / Health Information	Next of Kin Contact Information	Online / Instant Messaging Identifiers	Any form of correspondence
Relationship Status – marital / family relations	Photos, voice recordings, video footage, biometric data	Criminal Information	Physical / Postal Address
GENERAL PERSONAL INFORMATION – Company			
CIPC Documents	Directors / Shareholder Identification / Passport Details	Shareholding Certificates	Banking Details
Income Tax Reference	VAT Registration	Qualifications / Registrations / Memberships / Accreditations	BBBEE Certificate
Contact Details	Financial Statements / Bank Statements	Contactable References	Medical / Health Information

19. Transborder – Flow of Information

19.1. In compliance with PAIA Section 51(c)(iv), we inform you that our operations involve planned transborder flows of information within a secure Microsoft environment. This means that personal information may be transferred across international borders using Microsoft's cloud services and infrastructure. Microsoft ensures robust data protection and privacy measures, including compliance with international standards and regulations, to safeguard your information throughout these transborder data flows.

20. Security Measures

20.1. Safety SA Group have implemented a comprehensive set of security measures to protect personal information. These measures include, but are not limited to:

20.1.1. Encryption of data during storage and transmission.

20.1.2. Strict access controls to ensure only authorised personnel can access sensitive information.

20.1.3. Security audits to identify and address potential vulnerabilities.

20.1.4. Ongoing employee training programs to ensure awareness and adherence to data protection protocols.

20.2. These measures are designed to prevent: (a) Loss of, damage to, or unauthorised destruction of personal information. (b) Unlawful access to or processing of personal information.

20.3. By detailing these measures, Safety SA Group aim to fully comply with the requirements of PAIA and POPIA, providing a clear and transparent overview of how personal information is protected within our Microsoft environment.

21. Exercising Data Subject Rights under POPIA

21.1. Data Subjects may exercise any of the rights afforded to them under POPIA, including:

21.1.1. Request access to their Personal Information;

21.1.2. Request correction or updating of inaccurate or incomplete Personal Information;

21.1.3. Request deletion, destruction or de-identification of Personal Information where permitted by law;

21.1.4. Object to the processing of Personal Information;

21.1.5. Withdraw consent where processing is based on consent;

21.1.6. Request restriction of processing where applicable; and

21.1.7. Lodge a complaint regarding the processing of Personal Information.

21.1.8. Requests may be submitted through any of the following reasonably accessible channels:

21.1.9. By hand delivery: Porta Nova Building, Gazelle Close, Corporate Park South, Old Pretoria Road, Randjesfontein, Midrand, 1683

21.1.10. By post: Porta Nova Building, Gazelle Close, Corporate Park South, Old Pretoria Road, Randjesfontein, Midrand, 1683

21.1.11. By email: compliance@safetysa.com

21.1.12. Telephonically: +27872868222

21.1.13. By SMS or WhatsApp: +27 67 596 7993

21.1.14. Through any other reasonable communication channel made available by Safety SA Group.

21.2. Requests may be submitted free of charge during ordinary business hours.

21.3. Ordinary business hours are Monday to Friday from 08h00 to 17h00, excluding public holidays.

21.4. Safety SA Group may require reasonable proof of identity before processing a request.

21.5. Safety SA Group shall acknowledge receipt of the request and provide a written response within 30 calendar days unless an extension is permitted by law.

21.6. The outcome of the request shall be communicated in writing using the Data Subject's preferred communication channel where reasonably practicable.

21.7. Requests and objections received telephonically shall be recorded and retained by Safety SA Group as evidence of the request or objection.

21.8. Where a request or objection is received telephonically, the Data Subject may be requested to confirm the request in writing for verification purposes.

21.9. Prescribed POPIA forms, where applicable, may be obtained from the Information Regulator website or from the Information Officer.

22. Marketing and Communication

22.1. Safety SA Group may periodically contact data subjects to provide information about its events, seminars, products, services, and content that may be of interest, as well as to invite participation in research and projects. In accordance with applicable laws, if consent is required before sending certain types of marketing communications, Safety SA Group will only send such communications after obtaining explicit consent from the data subjects.

23. Availability of the Manual

23.1. A copy of the Manual is available online and at Safety SA Holdco for public inspection during normal business hours;

Physical Address	Porta Nova Building, Gazelle Close, Corporate Park South, Old Pretoria Road, Randjesfontein, Midrand, 1683

23.1.1. to any person upon request and upon the payment of a reasonable prescribed fee; and

23.1.2. to the Information Regulator upon request.