OBJECTIVE	To ensure legislative compliance
SCOPE	All Securi-Lid employees and Contractors.
AUTHORITY / RESPONSIBILITY	Human Resources
PROCEDURES	See below
DOCUMENTATION / REFERENCES	**Name:** Annexure 1 Annexure 2

1. DEFINITIONS

POPIA

Protection of Personal Information Act

Data Subject

Person to whom the personal information relates [natural or juristic person]

Responsible Person

The person who determines the purpose of and means for processing personal information

Operator

Person who processes personal information for a responsible person ito a contract/mandate, without coming under direct authority of that party

Processing

Anything that you can do with personal information including collection, storage, modification, destruction, etc.

2. INTRODUCTION

We are committed to compliance with The Protection of Personal Information (POPI) Act and will always:

- Sufficiently inform Data Subjects (customers/employees/contractors) of the specific purpose forwhich we will collect and process their personal information;
- Protect Personal Information from threats, whether internal or external, deliberate or accidental, to ensure business continuation, minimize business damage and maximize business opportunities.

This Policy establishes measures, processes, and standards for the protection and lawful processing of personal information.

The **Information Officer**, **Nikki Hornigold**, is responsible for:

- The monitoring of this policy;
- Ensuring that this policy is supported by appropriate documentation;
- Ensuring that this policy and subsequent updates are communicated to relevant managers, representatives, staff, and associates, where applicable.

All employees are responsible for adhering to this policy and for reporting any security breaches or incidents to the Information Officer.

Service Providers that provide IT and/or Off-site Data Storage services, to our organization must satisfy us that they provide adequate protection of data held by them on our behalf.

3. POLICY PRINCIPLES

Accountability for Data to be collected

- We shall take reasonable steps to safeguard all Data and Personal Information collected from customers, employees and contractors for the purpose of recruitment, sales, outsourcing etc.

Processing Limitation/Purpose for Data Collection

- We will collect personal information directly from customers, employees and contractors.
- Personal Information from Social Networks/Websites will be collectedwith the express consent of the Customer.

- Once in our possession, we will only process or further process customers, employee's or contactors information with their consent, except where we are required to do so by law. In the latter case, we will always inform the customer or employee.

Specific Purpose

- Personal information collected from customers, employees and contractors will be used for billing and contact purposes, both for customers, employees and contractors.

Limitation on Further Processing

- Personal information may not be further processed in a way that is incompatible with the initial purpose for which it was collected and will only be done with the express consent of the customer, employee or contractor.

Information Quality

- We shall ensure that all employee and customer information is complete, up to date, and accurate before we use it. We will request customers and employees, at least once annually, to update their information and confirm that we may continue to store/retain same.

Transparency/Openness

- Where personal information is collected from a source other than directly from a customer (E.g., Facebook, WhatsApp etc) we will make customers aware: (a) That their information is being collected and the specific reason; (b) Who is collecting their information by giving them our details.

Data Security Safeguards

- We will implement sufficient measures to guard against the risk of unlawful access, loss, damage, or destruction of personal information that is held:

    - physically
    - in our electronic database;
    - by a Data Storage Service Provider;
    - in any electronic devices (that will be Password protected).

- Data encryption of storage devices will be installed.

- We are committed to ensuring that information is only used for legitimate purposes with customer/employee/contractor consent.

Participation of Individuals/Complaints

- Customer/Employee/Contractors are entitled to access and correct any information held by us.
- Complaints should be submitted in writing to the Information Officer for Resolution.
- Requests to Access, Correct or Delete information must be made on the attached Annexures 1 and 2 and submitted to the Information Officer.

4. OPERATIONAL CONSIDERATIONS

Monitoring

- Management and the Information Officer are responsible for ensuring adherence to Standard Operating Procedures.
- All employees and individuals directly associated with business activities will be trained in the regulatory requirements governing the protection of Personal Information.
- We will conduct periodic reviews and audits, where appropriate, to ensure compliance with this policy and guidelines.

Policy Compliance

- Breach/es of this policy could result in disciplinary action and termination of employment.

5. ACCEPTABLE CHANNELS OF FORWARDING PERSONAL INFORMATION

Personal information can be dispatched either:

- Physically – In which case it is to be hand-delivered in a sealed envelope and will require the signature of the relevant recipient.

Or

- Emailed via our secured IT Platforms utilising MS Outlook and not through any 3rd party emailing software.

6. EXAMPLES OF DATA SUBJECTS

- Customers

- Permanent Employees
- Temporary Employees
- Contractors
- Suppliers

7. EXAMPLES OF PERSONAL INFORMATION

Includes but not limited to:

- Identity or passport number
- Date of birth and age
- Phone numbers
- Email address
- Physical address
- Gender, race and ethnic origin
- Disability
- Biometric data
- Marital relationship status
- Criminal record
- Private correspondence
- Employment history and salary
- Financial information
- Educational information
- Physical and mental health information

8. DIRECT MARKETING

The following provisions will apply with regards to direct marketing campaigns:

- The Company identifies and formulates a database of people (mostly dealerships) within the industry with the view to market its organisation.
- Existing clients and/or dealerships – we aim to market similar products and services.
- The Company undertakes to ensure opt-in and opt-out provisions are in place.
- New clients and/or dealerships – we undertake to obtain consent before any marketing material is sent through.

9. STORAGE

- Confirmation letter received in this regard, by TenacIT, our ISP & Network provider.
- Personal information collected is to be stored digitally, on a cloud-based service which is secured by TenacIT as well as physically in lockable filing cabinets which only HR & Finance have access to.
- Printing of documentation containing personal information is only to be done when absolutely necessary.
- Physical documentation containing personal information is to be filed immediately in secured filing cabinets with restricted access.

10. DESTRUCTION OF PERSONAL INFORMATION

- Securi-Lid will destroy hard copies that are stored physically, by ensuring that they are shredded in accordance with the guide on the retention of documents.
- Electronic copies that are stored in a protected cloud-based service such as Sage 300, will be deleted in accordance with the guide on the Retention of Documents.
- This guide is available upon request and will be monitored and complied with by the Information Officer.

11. BREACH OF SOP

Step 1

- Inform the Information Officer immediately.
- Secure personal information on the same day.

Step 2

- Complete an internal investigation within 24 hours and compile a report.

Step 3

- Inform Information Regulator as soon as possible.
- Inform Data Subject and Client where applicable.

Step 4

- Take corrective action to strengthen protocols and prevent future breaches.

ACKNOWLEDGEMENT

Please sign and return to the Director's Office

I hereby certify that I have read and understood Securi-Lid's POPIA Policy [Dated: 28 June 2021]

FULL NAME (PLEASE PRINT)	SIGNATURE	DATE

ANNEXURE 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [REGULATION 2]

NOTES:

1. Affidavits or other documentary evidence 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.

DETAILS OF DATA SUBJECT	
Name(s) and surname of data subject	
Unique identifier / Identity Number	
Residential, postal, or business address	
Contact number(s)	
E-mail address	

DETAILS OF RESPONSIBLE PARTY	
Name / Registered name of responsible party	
Residential, postal, or business address	
Contact number(s)	
E-mail address	

REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(D) TO (F)
Please provide detailed reasons for the objection below:

Signed at ……. this ……. day of …….. 20…….

……..…….

Signature of data subject / designated person

ANNEXURE 2

REQUEST FOR ACCESS TO/CORRECTION/DELETION OF PERSONAL INFORMATION OR DESTROYING/DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE POPI ACT, 2013 (ACT NO. 4 OF 2013) REGULATIONS, 2018 [REGULATION 3]

NOTES:

1. Affidavits or other documentary evidence 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.

Mark the appropriate request box with an X

	Access to/Correction or deletion of personal information about the data subject which is in possession or under the control of the responsible party.
	Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorized to retain the record of information.

DETAILS OF DATA SUBJECT	
Name(s) and surname of data subject	
Unique identifier / Identity Number	
Residential, postal, or business address	
Contact number(s)	
E-mail address	

DETAILS OF RESPONSIBLE PARTY	
Name / Registered name of responsible party	
Residential, postal, or business address	
Contact number(s)	
E-mail address	

INFORMATION TO BE ACCESSED/CORRECTED/DELETED/DESTROYED (Circle applicable request)
Give a description of Information:
Give detailed reasons for the request:

Signed at …… this ……. day of …….. 20…….

……..…….

Signature of data subject / designated person