PROVENPROTOCOL
Industrial Corporation

Protection of Personal Information Policy

INTRODUCTION

The purpose of this policy is to ensure that **PROVEN PROTOCOL (PTY) LTD**, being a private body complies, with its social and statutory obligations in terms of the protection of personal information and/or records which may be in its possession and/or come into its possession by virtue of the Company being a data subject, operator and/or responsible party.
This Policy also governs the processing of personal information by the Company.

RATIONALE

PROVEN PROTOCOL (PTY) LTD, making use of electronic communication, information matching programmes, biometrics and having in place one or more filing systems must seek to ensure that measures are taken to ensure compliance with relevant legislation as well as to ensure the protection of such personal information which is made known to the Company during the course of its operations.

DEFINITIONS

Words shall, for the most part, have the same meaning as that conveyed to them in terms of the Act, for the purposes of confirming such ascribed meaning, words with such specific definitions shall be italicised and in bold.

- "POPIA" shall mean the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), the Act shall have the same meaning.
- "PAIA" shall mean the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
- "Data Breach" shall mean any incident in which the personal information of any data subject is disclosed to unauthorized third parties.

LEGAL FRAMEWORK

This Policy is written in compliance with:

- The Protection of Personal Information Act, 2013, the Act;
- The Promotion of Access to Information Act, 2000, PAIA;
- The Regulations published in terms of the Act and PAIA.

SCOPE

- This policy applies to all Employees of **PROVEN PROTOCOL (PTY) LTD** (temporary and permanent) and also independent contractors, service providers and clients.
- All Employees, independent contractors, service providers and clients are required to fully understand and comply with the policy as contained in this document.
- **PROVEN PROTOCOL (PTY) LTD** reserves the right to monitor user activities for compliance, which monitoring may include any and all information stored- and/or accessed via the Company's telecommunications infrastructure.

APPOINTMENT OF INFORMATION OFFICER

- **PROVEN PROTOCOL (PTY) LTD** will ensure that an information officer and/or deputy information officer (as prescribed in terms of the Act) is duly appointed.
- Such information officer and/or deputy information officer shall be the responsible person for the purposes of this Policy and the Act and will ensure that pro-active measures are taken to ensure such compliance as may be required, both in terms this Policy and the Act.
- If no information officer and/or deputy information officer is appointed by the Company, the head of the Company shall be deemed to be the information officer until such a time as he/she has appointed such information officer and/or deputy information officer.
- The information officer and/or deputy information officer must be appointed by completing the relevant form as contained in:

Annexure A: Information Officer

Annexure B: Deputy Information Officer

It is herewith recorded that the Company has appointed:

Name of Information Officer: Koketso Mantholo Habedi
Contact email of Information Officer: koketso@provenprotocol.com
Contact number of Information Officer: 069 326 9850
as the Information Officer and any disclosures that need to be made to the Information Officer should be referred to this duly appointed Information Officer.

DUTIES OF INFORMATION OFFICER

It is the responsibility of the Information Officer and/or Deputy Information Officer to –

- Ensure that he/she is duly registered with the Information Regulator as required in terms of section 58(1) the Act;
- Ensure that the Company complies with its obligations under the Act;
- Interact with Heads of Department and such persons responsible for other Company Policies and Procedures to ensure that such documents, policies, procedures and systems comply with the provisions of the Act;
- Maintain this Policy and make sure that required amendments, revisions and addendums are made as- and when needed in order to comply with the Act;
- Ensure that interactions with clients of the Company occurs, in order to ensure that Agreements between the Company and its clients are updated in order to accommodate such changes as necessitated in terms of this Policy and/or by the Act (**See Annexure C**);
- Ensure that interactions with suppliers of the Company occurs, in order to ensure that Agreements between the Company and its suppliers are updated in order to accommodate such changes as necessitated in terms of this Policy and/or by the Act (**See Annexure D**);
- Ensure that the person(s) responsible for Human Resources within the Company implements changes to contracts of employment between the Company and its Employees in order to accommodate such changes as necessitated in terms of this Policy and/or by the Act (**See Annexure E**);

- Audit the electronic communication, information matching programmes, biometrics and filing systems of the Company in order to identify vulnerabilities as well as take adequate measures to mitigate such vulnerabilities;
- Ensure that the Company has the permission of Data Subjects to collect, store and process their Personal Information as contemplated in terms of sections 11(1)(f) and (2) of the Act;
- Engage the Company, Information Regulator and/or Data Subjects in the case of a Data Breach as required in terms of the Act;
- Ensure that any document or system which is used to collect the personal information of a data subject discloses to that data subject the lawful purpose for the collection of such personal information as contemplated in section 13 of the Act (**See Annexure J**);
- Ensure that personal information is not retained for longer than is necessary as contemplated in section 14 of the Act;
- Ensure that mechanisms and systems exist in order to comply with the Act, which includes, without limiting the generality of this duty, systems to de-identify, re-identify, and delete the data of qualifying data subjects; and
- Engage the relevant stakeholders of the Company in order to ensure compliance with the Act.

Notwithstanding the duties, the Information Officer remains ultimately responsible for the Company's compliance with the Act.

INVENTORY AND SECURITY OF SYSTEMS USED FOR THE STORAGE OF PERSONAL INFORMATION

HR Department:

Within the Human Resources Department, the following systems are in use for the purposes of conducting the Company's business:

- Employee Files (Including Contracts of Employment, Personal Information Sheets, Training Qualifications, Disciplinary Records, Banking Details, SARS Tax Details, Leave Forms, Medical Certificates, Polygraph Examinations, Residential Address, Contact Details, Next of Kin Details, Employment History, Pay Records, Regulatory Authority Membership Certificates, Medical Aid Membership, Provident Fund Membership etc.); and

- External Human Resources and/or Industrial Relations Provider(s)' systems which by necessity include access to information held by the Human Resources Department.
- In terms of securing the information within the Human Resources Department, which personal information is electronically recorded, or otherwise electronically stored on Computer systems, the control measures in place to safeguard such personal information are: **PROVEN PROTOCOL (PTY) LTD** out sources its maintenance and upkeep of computer systems to…**SMICT (PTY) LTD** ……who ensures that physical Security Measures are in place such as Antivirus, Firewall, Air-Gapping, Document Access Control, Directory Services (LDAP/AD Used for the management of users and passwords), etc.}
- In terms of securing the information within the Human Resources Department, which personal information is physically recorded, or otherwise exists as physical documents, the control measures in place to safeguard such personal information are: All personnel files are kept in locked offices, inside locked cabinets, Measures in place such as Access Control Registers, Alarm Systems and Armed Response.
- Retention period of information: Five years still after employee left the company

Finance Department:

Within the Finance Department, the following systems are in use for the purposes of conducting the Company's business:

- Accounting and/or Bookkeeping system;
- Online Banking Services;
- Payroll System
- Shift Scheduling System and
- SARS Online Services.
- In terms of securing the information within the Finance Department, which personal information is electronically recorded, or otherwise electronically stored on Computer systems, the control measures in place to safeguard such personal information are: **PROVEN PROTOCOL (PTY) LTD** out sources its maintenance and upkeep of computer systems to…… **SMICT (PTY) LTD** …… who ensures that physical Security Measures are in place such as Antivirus, Firewall, Air-Gapping, Document Access Control, Directory Services (LDAP/AD Used for the management of users and passwords), etc.}

- In terms of securing the information within the Finance Department, which personal information is physically recorded, or otherwise exists as physical documents, the control measures in place to safeguard such personal information are: All personnel files are kept in locked offices, inside locked cabinets, Measures in place such as Access Control Registers, Alarm Systems and Armed Response.
- Retention period: Ten years still after employee left the company

Operations:

Within the Operations of the Company, the following systems are in use for the purpose of conducting the Company's business:

- Access and Egress Registers (Physical or electronic register recording persons who enter and/or leave Company and/or Client Premises which record personal information of such persons);
- SHEQ Registers (COVID-19, Alcohol Testing, Induction, registers which record personal information);
- Equipment Registers (Such as firearms registers or other registers which record personal information);
- Vehicle Registers (Including pre-use checklists, vehicle registers and other documents which record driver information for the purposes of safeguarding such vehicles, including AARTO compliance);
- CCTV Camera Systems;
- In terms of securing the information within the Company's operations, which personal information is electronically recorded, or otherwise electronically stored on Computer systems, the control measures in place to safeguard such personal information are: ……**ATEX SOLUTIONS (PTY) LTD**…… provides assurance that they compliant to POPI act since 5 May 2021.
- In terms of securing the information within the Company's operations, which personal information is physically recorded, or otherwise exists as physical documents, the control measures in place to safeguard such personal information are: Physical Security Measures in place such as Access Control Registers, Control of physical Registers, Alarm Systems, Locks on offices and file cabinets, etc.}
- Retention period: As per company policy on document control.

Electronic Communications:

- The Company makes use of various electronic systems in order to communicate. Such electronic systems are used to distribute personal information within departments as well as to certain service providers (Industrial Law Service Providers, Employers' Organisations) and/or statutory authorities (Private Security Industry Regulatory Authority, Medical Aid Schemes, Provident Funds, Bargaining Councils, South African Revenue Services, etc.).
- The Company has taken reasonable measures to safeguard such personal information by virtue of securing its computer systems and networks as follows: **PROVEN PROTOCOL (PTY) LTD** uses a service provider ……**SMICT (PTY) LTD**…… that maintains the computer systems and ensures that physical Security Measures are in place such as Antivirus, Firewall, Air-Gapping, Document Access Control, Directory Services (LDAP/AD Used for the management of users and passwords).

Service Providers:

- Where the Company makes use of Service Providers who, by necessity, need access to the personal information of data subjects, such as attorneys, litigants, Labour Law Practitioners, Consultants and other such service providers, the Company has endeavoured to ensure the safeguarding of such personal information by virtue of confidentiality agreements prohibiting the disclosure of such personal information to unauthorized third parties.
- It remains the responsibility of the Company to ensure that such Service Providers complies with the regulations contemplated in the Act for the safeguarding of personal information.

ACTIONS IN THE CASE OF A DATA BREACH

- Any person who is made aware or otherwise becomes aware of any data breach must inform the Information Officer as soon as is possible and without undue delay.
- It is the duty of the Information Officer to take immediate steps, including:
- Informing the Information Regulator of the nature and extent of the data breach;
- Taking reasonable measures to investigate the nature and extent of the Data Breach;

- Taking reasonable measures to take steps to ensure that Data Subjects are informed of the Data Breach in terms of section 22 of the Act;
- Updating the Policies and Procedures of the Company, including this Policy, to address the Data Breach and ensure that it cannot happen again; and
- Engaging with Suppliers and/or Clients where applicable to give effect to the above steps, especially where such Data Breach occurred outside of the Company.

ACCESS TO PERSONAL INFORMATION BY DATA SUBJECTS

In the case where a data subject requests so, by virtue of completing the appropriate form – :

- Annexure F: Request for the Deletion of Personal Information;
- Annexure G: Request for the Disclosure of Personal Information held by the Company;
- Annexure H: Request for the Correction of Personal Information;
- Annexure I: Objection to the processing of Personal Information;

PROVEN PROTOCOL (PTY) LTD will take reasonable steps, where appropriate, to comply with the relevant request of the Data Subject if it is reasonable to do so, with specific emphasis on the Company's obligations and noting the Company's rights to process such personal information as contemplated in terms of section 11(1)(f) of the Act.

It remains the duty of the Company to consider any such application made by a Data Subject and respond to the Data Subject, indicating weather that the Company has complied with such request or, if applicable, the reason(s) why the Company did not comply with the request.