PROTECTION OF PERSONAL INFORMATION POLICY & PROCEDURE

Throughout this policy, any references to "the Company" should be interpreted as Extribyte Pty Ltd.

1. Purpose

1.1 The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 (hereafter referred to as "the POPI Act").

1.2 The Company aims to promote the protection of privacy through the processing of personal information in a context-sensitive manner.

1.3 Through the nature of its business, the Company is necessarily involved in the processing of personal information of employees, clients and other stakeholders.

1.4 A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

1.5 Given the importance of privacy, the Company is committed to effectively managing personal information in accordance with the POPI Act's provisions.

1.6 The purpose of this policy is to demonstrate the Company's commitment to protecting the privacy rights of employees, clients and other stakeholders in the following manner:

1.6.1 Through stating desired behaviour and directing compliance with the provisions of the POPI Act and best practice.

1.6.2 By cultivating a Company culture that recognises privacy as a valuable human right.

1.6.3 By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.

1.6.4 By creating business practices that will provide reasonable assurance that the rights of employees, clients and stakeholders as data subjects are protected and balanced with the legitimate business needs of the Company.

1.6.5 By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

1.7 It is important to note that the legal duty to comply with the POPI Act's provisions is activated in any situation where there is processing of personal information, entered into a record by or for a responsible person, who is domiciled in South Africa. This duty does not apply in situations where the processing of personal information is concluded in the course of purely personal or household activities, or where the personal information has been de-identified as defined in the POPI Act.

2. Processing of personal information

2.1 Personal information, in terms of the POPI Act and for the purposes of this policy, is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person (such as a Company), including, but not limited to information concerning:

- Race
- Gender
- Sex
- Pregnancy
- Marital status
- National or ethnic origin
- Colour
- Sexual orientation
- Age
- Physical or mental health
- Disability
- Religion
- Conscience
- Belief
- Culture
- Language

- Birth
- The education or the medical, financial, criminal or employment history of the person
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person
- The biometric information of the person
- The personal opinions, views or preferences of the person
- 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
- The views or opinions of another individual about the person
- 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.

2.2 "Processing" refers to processing as defined in the POPI Act and includes, but is not limited to the collecting, receiving, recording, organising, collating, storing, updating, retrieving, altering, using, disseminating, distributing, merging, linking, blocking, degrading, erasing or destroying of any personal information.

2.3 Due to the nature of the Company's business, the nature and requirements of the employment relationship, and the legal context that governs employment relationships, the Company needs to process employees' personal information as defined in the POPI Act. This includes, but is not limited to, processing:

2.3.1 For any purposes connected with the employee's employment, including but not limited to maintaining personal contact details, to comply with applicable legislation, payroll and remuneration, implementing health management systems, performance evaluation, training, development planning, occupational health and safety, security and access control, implementation of medical aid schemes and retirement funding, administration of benefits, to ensure employees proceed on sick leave and maternity leave when necessary, to protect employees' beliefs and culture, employment and credit references, succession and contingency planning.

2.3.2 In order to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

2.3.3 In order to protect the Company's legitimate interests as employer in respect of criminal offences which have been, or can reasonably expected to be, counted against the employee or other employees in the service of the Company.

2.4 From time to time, personal information may need to be processed by third parties as part of the employment relationship, including but not limited to, government departments, SETAs, professional bodies, etc. Employees are, therefore, required to consent to the processing, analysing and assessment of their personal information by any such third party, whether based in South Africa or in other jurisdictions. Any personal information will only be used by any such third parties in accordance with the provisions of this policy, and on instruction and consent of the Company.

2.5 Employees must warrant that any and all personal information provided by them to the Company shall at all times be true and correct, and that the provision of inaccurate and/or misleading personal information shall constitute serious misconduct, subject to appropriate disciplinary action, including potential dismissal.

3. Rights of employees, client and other stakeholders as data subjects

Where appropriate, the Company will ensure that its employees, clients and other stakeholders are made aware of the rights conferred upon them as data subjects, and that the Company gives effect to these rights:

3.1 The right to be informed that personal information is collected and/or processed.

3.2 The right to access personal information

3.2.1 The Company recognises that a data subject has the right to establish whether the Company holds personal information related to him or her and which information is being held, including the right to request access to that personal information.

3.2.2 A data subject may, at any time, request to know to whom his or her personal information has been disclosed.

3.3 The right to have personal information corrected or rectified

3.3.1 Data subjects have the right to request that their information be corrected or amended. They also carry joint responsibility in providing updated information when and where applicable, within a reasonable time period.

3.4 The right to erase

3.4.1 Data subjects have the right the request that their information be deleted or removed, subject to having legal standing and grounds for doing so, and subject to the Company's legal basis for processing information, and legal obligations related to the retention of information.

3.5 The right to restrict

3.5.1 Data subjects have the right to request that their information only be used for specific (restricted) purposes, subject to having legal standing and grounds for doing so, and subject to the Company's legal basis for processing information.

3.6 The right to object to the processing of personal information

3.6.1 The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

3.6.2 In such circumstances, the Company will give due consideration to the request and the requirements of the POPI Act.

3.6.3 The Company may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

3.6.4 A data subject has the right to object to the processing of his or her personal information for purposes of direct marketing by means of unsolicited electronic communications

3.7 The right against automated processing decisions

3.7.1 A data subject has the right to not be subject to decisions which affect him or her to a substantial degree and which are based solely on the automated processing of their information, with the exclusion of specifics as outlined by the POPI Act.

3.8 The right to be notified

3.8.1 The data subject also has the right to be notified in any situation where the Company has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

3.9 The right to register a complaint with the Information Regulator and the right to civil proceedings

3.9.1 Any complaints regarding the protection of personal information should be dealt with by way of internal processes first.

3.9.2 Thereafter, the data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under the POPI Act and to institute civil proceedings regarding the alleged non-compliance with the protection of his or her personal information.

4. General guiding principles

All employees and persons acting on behalf of the Company will at all times be subject to, and act in accordance with, the following guiding principles:

4.1 Accountability

4.1.1 Failing to comply with the POPI Act could potentially damage the Company's reputation or expose the Company to legal action, including a civil claim for damages. The protection of personal information is, therefore, everybody's responsibility.

4.1.2 The Company will ensure that the provisions of the POPI Act and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the Company will take appropriate sanctions, which may include disciplinary action, against those individuals who, through

their intentional or negligent actions and/or omissions, fail to comply with the principles and responsibilities outlined in this policy.

4.2 Processing limitation

4.2.1 The Company will ensure that personal information under its control is processed:

- In a fair, lawful and non-excessive manner.
- Only once the informed consent of the data subject has been received (unless another of the legal justifications in the POPI Act applies).
- Only for specific purposes.

4.2.2 The Company will under no circumstances distribute or share personal information with any person or entity that is not directly involved with facilitating the purpose for which the information was originally collected.

4.3 Purpose specification

The Company will process personal information only for specific, explicitly defined and legitimate reasons.

4.4 Further processing limitation

Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose, or consent to further processing has been obtained.

4.5 Information quality

The Company will take reasonable and practicable steps to ensure that personal information processed is complete, accurate, updated and not misleading.

4.6 Open communication

The Company will take reasonable steps to ensure that data subjects are aware that their personal information is being collected, including the purpose for which it is being collected and processed.

4.7 Security safeguards

4.7.1 The Company will manage the security of its systems to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

4.7.2 Security measures will also be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or bank details, the greater the security required.

4.7.3 The Company will continuously review its security controls (both technical and organisational) which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company's IT network.

4.7.4 The Company will ensure that all paper and electronic records comprising personal information are safely stored and made accessible only to authorised individuals.

4.7.5 All new employees will be required to sign employment contracts containing contractual terms for the use and storage of personal information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the Company is responsible.

4.7.6 The Company's operators and third-party service providers will be required to enter into service level agreements with the Company where both parties pledge their mutual commitment to the POPI Act and the lawful processing of any personal information pursuant to the agreement.

4.8 Data subject participation

4.8.1 A data subject may request the correction or deletion of his or her personal information held by the Company, in certain circumstances.

4.8.2 The Company will ensure that it provides a facility for data subjects who want to exercise their rights in terms of the POPI Act.

5. Employees and internal stakeholders who act on behalf of the Company

5.1 Employees and internal stakeholders who act on behalf of the Company will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.

5.2 Employees and internal stakeholders who act on behalf of the Company are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

5.3 Employees and other persons acting on behalf of the Company may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within the Company or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

5.4 Employees and other persons acting on behalf of the Company must request assistance from their manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

5.5 Employees and other persons acting on behalf of the Company will only process personal information where one or more of the following guidelines apply:

5.5.1 The data subject, or a competent person where the data subject is a child, consents to the processing.

5.5.2 The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party.

5.5.3 The processing complies with an obligation imposed by law on the responsible party.

5.5.4 The processing protects a legitimate interest of the data subject.

5.5.5 The processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the information is supplied.

5.6 Furthermore, the Company is only permitted to process personal information where the data subject clearly understands why and for what purpose his, her or its personal information is being collected and has granted the Company with explicit written or verbally recorded consent to process his, her or its personal information. These requirements are included in Company processes and documentation where required. It is, therefore, an obligation under this policy for all employees and other persons who

act on behalf of the Company, to ensure that they comply with all such process and documentation requirements.

5.7 Employees and other persons acting on behalf of the Company will under no circumstances:

5.7.1 Process or have access to personal information where such processing or access is not a requirement to perform their tasks or duties.

5.7.2 Save copies of personal information directly to their own private computers, laptops or other mobile devices such as tablets, smart phones, external hard drives, flash drives, etc. All personal information must be accessed and updated from the Company's central database or a dedicated server.

5.7.3 Share personal information informally.

5.7.4 Transfer personal information outside of South Africa without express permission from the relevant internal authority.

5.8 Employees and other persons acting on behalf of the Company are responsible for:

5.8.1 Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.

5.8.2 Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.

5.8.3 Ensuring that personal information that is sent or shared electronically, is done so in a safe and secure manner.

5.8.4 Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.

5.8.5 Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

5.8.6 Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs, that these are kept locked away securely when not being used.

5.8.7 Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it.

5.8.8 Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them.

5.8.9 Taking reasonable steps to ensure that personal information is kept accurate and up to date.

5.8.10 Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

5.8.11 Undergoing the POPI Act awareness training from time to time when it is made available by the Company.

5.9 Where an employee, or a person acting on behalf of the Company, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to their manager or the Information Officer.

5.10 All employees are required to take sensible and reasonable precautions to safeguard the security (cyber, online and other) of any information that is held by the Company. This includes not exposing the Company or its systems to cyber- and other information breach threats, through negligence or misconduct.

6. Version control

This policy and procedure document is reviewed once a year to ensure its continuing compliance with relevant regulations and legislation, as well as relevant internal changes in

strategy, priorities, practices, etc. A record of contextual changes, additions or omissions is given below.

Version*	Revision date	Effective date	Significant changes
V01-01-2020	1 April 2023	1 April 2022	New policy and procedure document

* The version number of the document will only be changed in the case of changes being made during the review process. Should no need for change arise during the review process, the version number will remain unchanged.