Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

PROTECTION OF PERSONAL INFORMATION ACT (POPIA) OF 2013 MANUAL

AKILI IT SERVICES (PTY) LTD

(Hereafter referred to as the Company)

Company Registration Number:	2018/603685/07
VAT Registration Number (*if applicable):*	4760217622
Physical Address:	6763 Seedcracker Street Celtisdal Centurion 0157
Name of Information Officer:	Mncedisi Chris Mabhele
Email Address of Information Officer:	chris@akili.co.za

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Internal Document Approval

Information Officer Name	Signature	Date
Mncedisi Chris Mabhele		20/11/2024

Document Version Control

Version	Date	Summary of Changes
1.0	29/06/2021	Original version
2.0	01/11/2024	Data encryption
3.0	20/11/2024	Annexures related to Microsoft

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Index

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

SECTION 1: PARAMETER DECLARATION

1.1. Definitions

Term	Definition
Backup	Means the copying of physical or virtual files or databases to a secondary location for preservation to assist in the event of equipment failure or catastrophe.
Biometrics	Means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition (*Section 1 of the Protection of Personal Information Act 4 of 2013).*
Bring your own Device (BYOD)	Bring your own Device is the practice of allowing employees and other authorised persons that perform work for the Company to use their own personal devices for work purposes. This includes mobile phones, laptops, and tablets.
Business day	Shall mean any day other than a Saturday, Sunday, or Public Holiday in terms of the laws of the Republic of South Africa.
Child	Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself (*Section 1 of the Protection of Personal Information Act 4 of 2013).*
Company	Shall mean Akili IT Services (Pty) Ltd as specified on the Title page of this document.
Confidential Information	Confidential Information is a broader category than Personal Information (*Please refer to the definition of Personal Information*). This means that, as a rule, all Personal Information is confidential and should be kept confidential, but not all Confidential Information is necessarily Personal Information. Confidential means to be entrusted with another person's confidence or secret affairs.
Consent	Consent means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of Personal Information. (*Section 1 of the Protection of Personal Information Act 4 of 2013)*
Consumer	Shall mean any individual, client, customer, company, or any other legal entity making use of the services of the Company
Controls	Means control measures put in place by the Company to mitigate the risks identified to the security of Personal Information and / or Confidential Information, including instituting and implementing policies and procedures, management control, reporting, physical security measures and the like.
Data	Information that is entrusted with another person's confidence or secret affairs.
Data breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Data Subject/s	Data subject means the person or business to whom personal information relates (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Data Subject Category	For Juristic and Natural Persons examples: customer/client category; supplier/service provider category; employee category; other (e.g., shareholders; members; stakeholders; non-executive directors).
Desk/s and Table	Means any physical working area where Personal Information and / or Confidential Information is processed, including printing areas, whether situated at the Company's premises or remotely.
Direct Marketing	Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject or requesting the data subject to make a donation of any kind for any reason (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Electronic Communication	Means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient (*Section 1 of the Protection of Personal Information Act 4 of 2013).*
Filing System	POPI only applies to the processing of Personal Information which is in a record which forms part of a filing system. It is therefore important to know what a filing system is. A filing system is any structured set of Personal Information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria (*Section 1 of the Protection of Personal Information Act 4 of 2013).*
Information Incident	This means a single or a series of unwanted or unexpected events that threaten information security or privacy. Information Incidents include any collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorised by the Company or the owner of such information (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Information Matching Programme	Means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject (*Section 1 of the Protection of Personal Information Act 4 of 2013).*
Information Officer	A Person appointed to implement the protection of the privacy of Personal Information in a Responsible Party or Company and the compliance of the POPI Act (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Information Regulator / the Regulator	There is hereby established a juristic person to be known as the Information Regulator, which: • Has jurisdiction throughout the Republic. • Is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour, or prejudice. • Must exercise its powers and perform its functions in accordance with this Act and the Promotion of Access to Information Act. • Is accountable to the National Assembly. (*Section 39 of the Protection of Personal Information Act 4 of 2013)*
ISO27000 Series	Means the international standard for implementing an information security management system.
IT User	Means a User (*Please refer to the definition of User*) within the Company, authorised to be responsible for the carrying out of the Company's necessary Information Technology functions.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Juristic Person	Legal entity, e.g., company, close corporation, business trust, homeowner's association, state-owned entity (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Natural Person	Human being, e.g., sole proprietor, partners (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Operator	An operator means a person who processes Personal Information for or on behalf of a Company in terms of a contract or mandate, without coming under the direct authority of that party (*Section 1 of the Protection of Personal Information Act 4 of 2013)*
Personal Data	Personal data is any Information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers.
Personal Data Breach	A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored, or otherwise processed.
Personal Information	Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including: • Information relating to the 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. • Information relating to 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 assignment to the person. • The biometric information of the person. • The personal opinions, views, or preferences of the person. • Correspondence sent by the person. • 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. *(Section 1 of the Protection of Personal Information Act 4 of 2013)*
Policy	A Statement that sets out the scope within one operates, it confirms what one can do, e.g., Privacy Policy.
Premises	The Company's premises or physical address, as per the Title Page of this document.
Procedure	A Statement that sets out how one implements a Policy, e.g., how the business activities functions, and practices could be the Privacy Impact Assessment Procedure.
Processing	Processing means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including • The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use. • Dissemination by means of transmission, distribution or making available in any other form. • Merging, linking, as well as restriction, degradation, erasure, or destruction of information. (*Section 1 of the Protection of Personal Information Act 4 of 2013)*

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Public Record	A public record is a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether it was created by that public body. (*Section 1 of the Protection of Personal Information Act 4 of 2013)*
Record	A record is any recorded Information regardless of form or medium: • Writing on any material. • Information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, and other device. • Any material subsequently derived from information so produced, recorded, or stored. • Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means. • Book, map, plan, graph, or drawing. • Photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced. • In the possession or under the control of a responsible party. • Whether or not it was created by a responsible party. • Regardless of when it came into existence. (*Section 1 of the Protection of Personal Information Act 4 of 2013)*
Responsible Party	A Responsible Party is a body or person who determines the purpose of and means for processing Personal Information. Included in this definition are juristic persons (e.g., companies and businesses), whether they are public or private organisations (*Section 1 of the Protection of Personal Information Act 4 of 2013)*. For purposes for this manual “the Company” is deemed the “the Responsible Party”
Restoration	This means the process of restoring something to its former condition. In the case of a computer or other electronic device, means returning it to a previous state, including restoring a previous system backup or the original factory setting, or restoring data that was on the system.
Screen/s	This means any monitor on any device upon which Personal Information and / or Confidential Information is stored that displays such information.
Security Incident	Security Incident means any actual or potential accidental or unauthorised access, destruction, loss, alteration, disclosure, or any other unlawful forms of processing of Personal Information by the Company.
Special Personal Information	Special personal information means: • The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. • The criminal behaviour of a data subject (*Section 26 of the Protection of Personal Information Act 4 of 2013)*
Security safeguards	The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent: • loss of, damage to or unauthorised destruction of personal information. • unlawful access to or processing of personal information. The responsible party must take reasonable measures to:

	• identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control. • establish and maintain appropriate safeguards against the risks identified. • regularly verify that the safeguards are effectively implemented. • ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations. (*Section 19 of the Protection of Personal Information Act 4 of 2013)*
Unique Identifier	Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party (*Section 1 of the Protection of Personal Information Act 4 of 2013)*.
Users	This is the employees, contractors, visitors, and / or other persons authorised to access and use the Company's systems
Website	A website is a collection of web pages and related content that is identified by a common domain name and published on at least one web server. Notable examples are Wikipedia.org, Google.com, and Amazon.com. All publicly accessible websites collectively constitute the World Wide Web.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

1.2. List of Abbreviations

Abbreviation	Term
BYOD	Bring Your Own Device
CEO	Chief Executive Officer of the Company
CIO	The Chief Information Officer of the Company
CPA	The Consumer Protection Act 68 of 2008
DPA	United Kingdom Data Protection Act of 1998
DRP	Disaster Recovery Plan
DSAR	Data Subject Access Requests
ECTA	Electronic Communications and Transactions Act 25 of 2002
FICA	Financial Intelligence Centre Act, 2001
GDPR	The General Data Protection Regulation of the European Union
IAO	Information Asset Owner
IT	Information Technology and Communications Systems
NCA	National Credit Act 34 of 2005
PAIA	Promotion of Access to Information Act, Act 2 of 2000
PAJA	Promotion of Administrative Justice Act 3 of 2000
POPIA	Protection of Personal Information Act 4 of 2013
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002
SDI	Spatial Data Infrastructure
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

1.3. Applicable National Legislation

The Company recognizes that the Protection of Personal Information Act (POPIA) of 2013 does not exist in isolation and that POPIA acknowledges various rights regarding the processing of personal information in National legislation. The daily operations of this Company areas of compliance in the following:

(Please note that the Company needs to assess which legislation is applicable to it and the list below is just an example for ease of reference.)

Please mark the relevant legislation to the Company with an x.

National Legislation

x	National Legislation
X	Basic Conditions of Employment Act No 75 of 1997
X	Bill of Rights of 1993
	Child Care Act 74 of 1983
	Children's Act 38 of 2005
	Children's Amendment Act 41 of 2007
	Civil Aviation Offences Act 10 of 1972
	Close Corporations Act No 69 of 1984
	Companies Act No.61 of 1973
X	Companies Act No 71 of 2008
X	Compensation for Occupational Injuries and Diseases Act, No. 130 of 1993
X	Constitution of the Republic of South Africa 1996
	Consumer Protection Act 68 of 2008
	Co-Operatives Act No.91 of 1981 Section 237
X	Copyright Act No 98 of 1978
	Correctional Services Act 111 of 1998
X	Criminal Procedure Act 51 of 1977
	Customs and Excise Act 91 of 1964

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

	Customs Control Act 31 of 2016
X	Cybercrimes and Cybersecurity Bill of 2017
	Deeds Registries Act, No. 47 of 1937
X	Electronic Communications Act 36 of 2005
X	Electronic Communications and Transactions Act 25 of 2002 (ECTA)
X	Employment Equity Act No 55 of 1998
	Environment Conservation Act, No. 73 of 1989
	Extradition Act 67 of 1962
	Financial Advisory and Intermediary Services Act No 37 of 2002
	Financial Intelligence Centres Act 38 of 2001
	Firearms Control Act, No. 60 of 2000
	Guidance and Placement Act 62 of 1981
	Harmful Business Practices Act 70 of 1988
X	Income Tax Act No.58 of 1962, Sections 75(1) and (2).
X	Income Tax Act No 95 of 1967
	Insolvency Act No.24 of 1936
	Labour Relations Act No 66 of 1995
	Long Term Insurance Act, No. 52 of 1998
	Maintenance and the Promotion of Competition Act 96 of 1979
	Mutual Banks Act No.124 of 1993
	National Archives and Record Services Act, 43 of 1996
	National Credit Act 34 of 2005 (NCA)
	National Prosecuting Authority Amendment Act 56 of 2008
	National Road Traffic Act, No. 93 of 1996
	Nuclear Energy Act 46 of 1999
X	Occupational Health and Safety Act, No. 85 of 1993

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

	Prescription Act No.68 of 1969
	Prevention and Combating of Hate Crimes and Hate Speech Bill of 2016
	Prevention and Combating Trafficking in Persons Act 7 of 2013
	Prevention of Organized Crime Act 121 of 1998
X	Promotion of Access of Information Act No 2 of 2000
	Promotion of Administrative Justice Act 3 of 2000 (PAJA)
	Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000 (PEPUDA)
	Protected Disclosures Act, No. 26 of 2000
X	Protection of Access to Information Act 2 OF 2000 (PAIA)
	Protection of Constitutional Democracy against Terrorist and related Activities Act 33 of 2004
	Public Finance Management Act 1 of 1999
	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA)
	Sale and Service Matters Act No. 25 of 1964
	Second Hand Goods Act No. 23 of 1955
	Short Term Insurance Act, No. 53 of 1998
	Skills Development Act, No. 97 of 1997
	Skills Development Levy Act, No. 9 of 1999
	South African Police Services Amendment Act 57 of 2008
	South African Revenue Services Act 34 of 1997
	Spatial Data Infrastructure Act 54 of 2003 (SDI Act)
	Stamp Duties Act No.77 of 1968, Section 23(6).
	STANSA 15489, South African Standard for Record Management
	Stock Exchange Control Act No.1 of 1985
	Tax Administration Act 28 of 2011
	Tobacco Products Control Act, No. 12 of 1999

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

	Trademarks Act 194 of 1993
	Transfer Duty Act, No. 40 of 1949
X	Unemployment Insurance Act No 30 of 1996
X	Value Added Tax Act No 89 of 1991
Specify any other legislation of international regulation:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

SECTION 2: PRIVACY STATEMENTS AND APPOINTMENTS

2.1. POPIA Privacy Policy Statement

In South Africa, consumers have a deep mistrust and lack the confidence that organisations use the information they collect lawfully and for an agreed upon purpose. The Protection of Personal Information Act (POPIA) of 2013 is South Africa's new data protection law. It joins a raft of similar laws around the world.

We, the Company, believe the consumer privacy is something that they never have to question. It should be simple, straightforward, and understood. Therefore, the Company builds its Privacy Policy Statement on these three objectives:

- Respect for consumer privacy.
- Provision of transparency on information processing.
- Provision of security as it relates to cybertheft, data loss and identity theft.

We believe that privacy should be focused on private consumer interactions, data encryption, reducing data permanence, data safety, interoperability of devices and applications, and secure data storage. We take full responsibility in terms of the Protection of Personal Information Act of 2013 (POPIA) to take reasonable measures to ensure data security and prevent data breach or loss.

POPIA is about security, is addition to being about respecting the rights of the data subject.

The Company shall promote a culture of data privacy and digital transformation as a vital strategy in the complexity of our daily operations. This would deliver a competitive advantage to the Company soon. The Company acknowledge that there is no single tool that can accomplish end-to-end POPIA compliance, but that it is only possible through the ethical conduct of employees and managers, and the security and maintenance of our data protection systems.

Akili is committed to protecting the privacy and confidentiality of Microsoft personal data processed, stored, or transmitted in collaboration with Microsoft services. To ensure compliance with industry standards and regulatory requirements, we fully adhere to the principles and guidelines outlined in the Microsoft Privacy Statement

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

_____

Information Officer Signature

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

2.2. The Appointment of an Information Officer

An Information Officer must be formally appointed within the Company. The Information Officer must be registered with the Information Regulator as per Section 55 of POPIA. The Information Officer is accountable and liable for the lawful processing of data within the Company. The Information Officer must thereby be an Executive within the Company, such as the CEO.

(*Refer to: Section 1 of the Protection of Personal Information Act 4 of 2013; Sections 1, 17 of the Promotion of Access to Information Act 2 of 2000)*

The Information Officer various responsibilities in terms of POPIA as well as PAPIA. The Information Officer has control over why and how personal information is processed within the Company, including decisions such as:

- To collect the personal information and whether there is a legal basis for the collection.
- Which personal information to collect.
- What the personal information will be used for.
- Whose personal information will be collected.
- Whether to disclose the personal information and to whom.
- Whether to give data subjects access to their personal information.
- How long to keep the personal information.
- Whether to make non-routine amendments to the personal information.

The duties of the Information Officer are listed as below (*Refer to: Section 55(1) (a-e) of the Protection of Personal Information Act 4 of 2013)*:

- Bring the Company into compliance with the POPIA.
- Develop a policy on how the Company should implement the lawful processing of personal information.
- Issue notices and train and encourage employees to implement lawful processing of personal information.
- Provide a reasonable opportunity to consumers to conform to Data Subject Access Requests (DSAR) process, where any reasonable DSAR request will not be denied or rejected.
- Oversee, monitor, and govern DSAR request processing.
- Ensure the POPIA Compliance Framework is developed, implemented, monitored, and maintained.
- Develop and maintain a PAIA manual, if necessary.
- Develop measures to process DSAR requests for information access.
- Conduct internal POPIA awareness training.
- Support the Information Regulator in their investigations.
- Submit to the Information Regulator an annual report on activities related to POPIA compliance, as requested by the Information Regulator.

The Enforcement Committee of the Information Regulator may recommend action against the Information Officer under the POPIA and PAIA. The Information Officer may be held criminally liable for the offence in respect to any breach of the provision of the POPI Act or PAIA. Penalties could include a fine or imprisonment not exceeding 2 to 3 years, depending on the offence.

For the Online Registration of the Responsible Party's Information Officer:
https://www.justice.gov.za/inforeg/portal.html

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (2.2) A: INTERNAL INFORMATION OFFICER APPOINTMENT FORM

I hereby and with immediate effect, appoint you:

Full Name and Surname:	Mncedisi Chris Mabhele
ID Nr:	780915 5753 087

as the Information Officer, as required by the Protection of Personal Information Act (POPIA 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the Company's reasonable compliance with the provisions of POPIA.
- Keeping management updated about the Company's information protection responsibilities under POPIA.
- Continually analysing regulations and aligning them with the Company's personal information processing procedures.
- Reviewing the Company's information protection procedures and related policies.
- Ensuring POPIA audits are scheduled and conducted on a regular basis.
- Ensuring that the Company makes it convenient for consumers and data subjects who want to update their personal information or submit POPIA related complaints to the Company.
- Approving any contracts entered to with operators, contractors, service providers, employees, and other third-parties which may have an impact on the personal information held by the Company.
- Overseeing the amendment of the Company's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the Company, are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company's security controls.
- Organising and overseeing awareness training of employees and other individuals involved in the processing of personal information on behalf of the Company.
- Addressing employees' POPIA related queries.
- Addressing all POPIA related requests and complaint made by the Company's data subjects.
- Working with the Information Regulator in relation to ongoing investigations. The Information Officer will therefore act as a contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, regarding any other matter.

Board Members Name and Signature:

Mncedisi Chris Mabhele

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ACCEPTANCE

I Mncedisi Chris Mabhele understand the implications of the appointment and confirm my acceptance of this appointment. I have studied the relevant sections of the POPIA and associated Regulations and understand what is required of me.

Full Name and Surname:	Mncedisi Chris Mabhele
Date:	29/06/2021
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

2.3. Website Privacy Statement

To be placed on the Company Website

2.3.1. COMMITMENT TO YOUR PRIVACY

Welcome to the Website, owned and operated by the Company. The Company is committed to protecting the privacy of the user of the website. The Company values the trust of its subscribers and all others who work with it. The Company recognises that maintaining your trust requires transparency and accountability in how the Company handles your personal information. This privacy statement is incorporated into and is subject to the Company's standard Terms and Conditions relating to the use of the Website.

In performing the Company's services in the ordinary course of business, the Company may collect, use, and disclose personal information. Anyone from whom the Company collects such information can expect that it will be lawfully protected as far as reasonably possible and that any use of this information is subject to consent, as required by law. This is in line with the general privacy practices of the Company.

We comply with the Protection of Personal Information Act No. 4 of 2013 (POPIA) and the principles outlined in Sections 50 and 51 of the Electronic Communications and Transactions Act No.25 of 2002 (ECTA) which govern your right to having your personal information kept private.

This privacy statement sets out how the Company collects, uses, discloses, and safeguards the Personal Information it processes during its business.

2.3.2. DEFINITIONS

In this privacy statement the Company makes use of the following terms:

- *"Personal Information"* means all information which may be personal in nature or information about an identifiable natural or existing juristic person in terms of POPIA.
- *"User, you, your or yourself"* refers to any person who makes use of the Website.

2.3.3. WHAT PERSONAL INFORMATION DOES THE COMPANY COLLECT AND WHY?

The Company may collect personal information in conducting its ordinary business operations, including using its Website. In processing such personal information, the Company ensures that it complies with the provisions of POPIA, and personal information is used for legitimate business purposes.

The Company limits the use and disclosure of personal information to include only what is permitted in terms of POPIA, where consumers have consented to such collection, use and disclosure.

Confidentiality of your personal information is important to us. Unless we have your consent or permitted under the national laws, we will not sell, rent, or lease your personal information to others. We will not use or share your personal information in ways unrelated to the circumstances described in this Website Privacy Statement.

2.3.4. OBTAINING CONSENT

The Company does not, except where otherwise permitted by law, collect, use, or disclose your personal information without your consent.

2.3.5. USE AND DISCLOSURE OF PERSONAL INFORMATION

The Company operates its Website, and conducts its business in general, in accordance with South African legislation. The Company considers it imperative to protect the privacy interests of data subjects. If the Company sends personal information outside of South Africa (including if such information is hosted offshore), the Company will ensure that it takes all reasonable steps to ensure that it complies with all applicable laws in this regard, including POPIA.

Unless permitted under the law or your consent is obtained, the Company will not transfer your personal information outside the Republic of South Africa.

2.3.6. RETENTION OF PERSONAL INFORMATION

All personal information retained on the Company's database, including such information obtained using the Website, is in accordance with the retention provisions set out in the laws and regulations of South Africa, including those set out in POPIA.

We retain your personal information for as long as reasonably necessary to fulfil the purpose for which it was collected and to comply with laws and your consent to such purpose, remains valid after termination of our relationship with you.

2.3.7. YOUR RIGHTS IN RELATION TO YOUR PERSONAL INFORMATION

It is important to note that you have rights in relation to your personal information. You have the right to contact the Company at any time to ask the Company to:

- Confirm that it holds your personal information.
- Provide you access to any records containing your personal information or a description of the personal information that the Company hold about you.
- Confirm the identity or categories of third parties who have had, or currently have, access to your personal information.

The Company aims to ensure that your personal information is accurately recorded. To be able to achieve this, we adhere to processes that help ensure and maintain data accuracy. We provide individuals with reasonable access to review and correct their personal information. The Company's contact information is as set out on the Contact Us page of this Website.

When you make a request regarding your personal information, the Company will take reasonable steps to confirm your identity. There may be times when the Company cannot grant access to your personal information, including where granting you access would interfere with the privacy of others, or result in a breach of confidentiality. The Company will always provide you with reasons if this is the case.

If you are of the view that any personal information that the Company holds about you is incorrect, including that it is inaccurate, irrelevant, outdated, incomplete, or misleading, you can ask the Company to correct it. If you believe that any personal information that the Company holds about you is excessive or has been unlawfully obtained, you can ask the Company to destroy or delete it.

You may do the same if you think that the Company has retained if for longer than necessary, given the purpose.

It is important, however, to understand that if you withdraw your consent for the Company to use some of your personal information, it may affect the quality and level of service that the Company can provide to you.

When you contact the Company, please let us know your name, address, any email address you have provided and a description of the circumstances under which you provided the data. We will make reasonable efforts to incorporate as soon as practicable the changes in personal information that we maintain.

You have the right to lodge a complaint to the Information Regulator:

- By e-mail: inforeg@justice.gov.za
- To the following postal address: SALU Building, 316 Thabo Sehume Street, Pretoria.
- By telephone: 012 406 4818
- By Fax: 086 500 3351.

2.3.8. SECURITY

The Company takes security and the protection of personal information seriously. We maintain physical, technical, and organisational safeguards to protect any data that we collect. We have adopted procedures to secure storage of personal information and are committed to working with our data suppliers to protect the security of personal information during any transfer to or from us.

We have also instituted safeguards to identify and help prevent the fraudulent use of personal information. Your personal information is only accessible to those employees, agents, or contractors for business purposes and on a strictly need-to-know basis. For security purposes we then move all the personal information that we collect or obtain about you, to an environment on our network that has controls in place to limit access to and secure the data.

On the Website, we take precautions to secure your personal information. If we ask you to provide your personal information, we will do so through a web page that uses the industry standard secure transport protocol. This protocol provides security for your information by encrypting it as it travels from your computer to our computer.

To protect your privacy and security, we will also take reasonable steps to verify your identity before granting access to or making alterations to data we maintain.

The Company has adopted a security model to protect your personal information that complies with generally accepted information security practices and procedures. As part of the Company's security systems, the Company has implemented fire-wall technology, password controls, encryption processes and antivirus software. This is in addition to as the physical security measures adopted by the Company to ensure that it takes all reasonable technical and organisational measures to prevent loss of damage to, or unauthorised destruction of personal information, and unlawful access to or processing of personal information. The Company has a security policy in place that every employee, and supplier of the Company must adhere to.

2.3.9. CHILDREN'S PRIVACY

The Company defines children as individuals under the age of 18. This Website is not intended for the use of children, and we do not intend to collect information about children through the Website. This Company does not knowingly collect information from children under the age of 18 and our Website do not target children under 18. We encourage parents and guardians to take an active role in their children's online activities and interests.

You must be at least 18 to access or use any products or services through the Website or become a subscriber of any program entitled to subscription benefits.

2.3.10. COOKIES

The Website uses cookies in a limited way. Cookies are small files containing information that a Website uses to track a visit by a user. The Company uses session cookies to better understand how the Website is used by users to improve the performance of the Website for users.

A cookie is also set on your computer to allow the Company to recognize you whenever you visit and collect information, like the pages you visit and the preferences you choose. We use the information we collect for statistical purposes and to study how the Website is used so that we may improve and enhance your experience on the Website. No personal information is stored in cookies.

It is possible for you not to accept our cookies while using Website by setting the preference in your web browser.

If you would like more information about cookies, you can visit:
http://www.cookiecentral.com/n_cookie_faq.htm.

2.3.11. THIRD-PARTY WEBSITES

The Company Website may offer links to third-party websites, including payment gateways for credit card payment. You should be aware that operators of linked websites may also collect your personal information (including information generated using cookies) when you link to their websites. If you follow a link to any of these websites, it is important to note that these websites have their own terms of use and privacy policies and that the Company does not accept any responsibility or liability for them.

As the Company is not responsible for any representations, information, warranties, or content on any website of any third-party. The Company does not exercise control over third-parties' privacy policies. The Company is not responsible for how such parties collect, use, or disclose your information. It is important for you to familiarize yourself with their privacy policies before providing them with your personal information.

The Company may use Google Analytics or other similar analytical tools to obtain information collected to display, optimise, and personalise advertisements and customer experience on our Website. To determine which advertisements you may find useful, and to personalise your experience on the Website.

2.3.12. MARKETING

With your consent, the Company may use your personal information to promote and market additional products, services, and special offers from us or our affiliates that may be of interest to you. When you visit the Website, we may ask you if you want to sign-up to receive information and promotional offers and its marketing partners.

If you decide to register for emails, you may opt-out from receiving such communications, at any time. If you wish to opt-out, please contact us as per the details provided on the Contact Us page. If you do not provide us your consent, some features in our Website may not be available to you.

We will use your personal information for the direct marketing purpose only if you give your consent to us or it is permitted by the laws.

In case you no longer want to receive this news or information, you may opt-out of receiving such by responding to the newsletter and asking to be unsubscribed or calling the Company and asking to be taken off the list.

2.3.13. UPDATING OF PRIVACY POLICY

Our compliance with this Website Privacy Statement will be monitored on a regular basis. The Company reserves the right to modify this Website Privacy Statement with or without notice. The Website Privacy Statement posted at any time via the Website shall be deemed to be the Website Privacy Statement then in effect. You therefore agree and undertake to review the Website Privacy Statement whenever you visit the Website.

2.3.14. CONTACT INFORMATION

Questions, concerns, or complaints related to this Website Privacy Statement or the Company's treatment of personal information should be directed to the email address as per the Website Contact Us page.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

2.4. Terms and Conditions of Use for the Website

To be placed on the Company Website

2.4.1. INTRODUCTION

Welcome to the Website, owned and operated by the Company. These Terms and Conditions of use set out the terms that regulate the use of the Website by the user.

2.4.2. ACCEPTANCE OF TERMS

These Terms take effect as soon as you access the Website and is a binding agreement between the Company and yourself. The current version of these Terms will govern both the Company's and your rights and obligations each time you access this Website. If you do not agree with any provision contained in these Terms, you must immediately stop using the Website. Your failure to do so, and your continued use of the Website, will mean that you have read, understood, and agree to the provisions of these Terms.

2.4.3. USE OF THE WEBSITE

By accessing the Website, you warrant that your use of the Website is for lawful purposes, you are over 18 years of age, and you can legally conclude an agreement with the Company.

You further warrant that you will not contravene any South African or international laws by using the Website, any services offered on the Website, or any information provided to you by the Company through your use of the Website. Except as expressly authorised by these Terms, you may not use, alter, copy, distribute, or transmit any content contained on this Website.

2.4.4. USE OF INFORMATION

The Company conducts its business in accordance with South African legislation applicable to its business. One aspect of such legal compliance relates to data protection. The Company values the privacy of your information and will protect your personal information in accordance with laws and regulations. This includes the Protection of Personal Information Act no 4 of 2013 (POPIA).

By using the Website, you acknowledge, agree and consent to the Company and our suppliers, or any person authorised on our behalf, using your personal information, for any purpose necessary for you to use the Website, or for the Company to render any service to you via the Website.

2.4.5. AMENDMENT OF TERMS

The Company reserves the right to amend these Terms at any time. Whenever the Company concludes any amendments to these Terms, the amended Terms will be posted on this page, together with an indication at the bottom of the page as to the date upon which the Terms were last revised. You agree to review these Terms for any such amendments whenever you visit the Website. Should you not agree to any amendments to these Terms, you must immediately stop using the Website.

2.4.6. CONTENT OF USERS (If applicable)

There are certain areas on the Website that allow users of the Website to upload questions, data, and other information. As a user, you are responsible for the content that you upload, display, and add to the Website. The Company will not review any user content.

You agree not to add any user content that contains any information that is not legally permitted, you do not have a right to make available under any law, or under contractual relationships and you know is incorrect. You agree that any user content that you add to the Website does not violate any third-party rights.

2.4.7. COPYRIGHT AND INTELLECTUAL PROPERTY RIGHTS

For purposes of these Terms, Intellectual Property Rights means all intellectual property rights including, patents, designs, copyright, trademarks, trade secrets and know-how, applications and registrations, renewals, and extensions.

Unless the contrary is specified in these Terms, all content contained on the Website, or incorporated or embedded in any service offered on the Website, including software, images, text, graphics, illustrations, logos, branding, photographs, and all Intellectual Property Rights in such content, belongs exclusively to the Company. You agree that you will at no time lay claim to the Company content, and to any Intellectual Property Rights subsisting in such content.

Except as explicitly provided herein, nothing in these Terms shall be deemed to create a license to any Intellectual Property Rights belonging to the Company, and you agree that you will not:

- Modify, port, translate, localise, or create derivative works of the Company content.
- Decompile, disassemble, reverse engineer, or attempt to reconstruct, identify, or discover any source code, underlying ideas, underlying user interface techniques or algorithms contained or incorporated in any Company content.
- Disclose any of the Company content.
- Sell, lease, license, sublicense, copy, market, reproduce, transmit or distribute the Company content.
- Knowingly take any action that would cause any of the Company content to be placed in the public domain.

You understand and acknowledge that you may be exposed to user content that is inaccurate, misleading, and offensive. You agree that the Company will not be liable for any damages you allege to incur because of exposure to such user content.

2.4.8. DISCLAIMER OF WARRANTIES AND LIABILITIES

The Company does not make any warranties, statements, or guarantees, regarding the Website and any services offered on the Website. These are provided on an "as is" basis. Use of the Website, any Company content and any service offered is entirely at your own risk.

The Company makes no warranties or conditions about the quality, accuracy, reliability, completeness, or timeliness of any of the foregoing. The Company does not take any responsibility for any errors, omissions or inaccuracies on the Website, the content and any service that may be offered.

Neither the Company nor its shareholders, directors, or employees (Indemnified Parties), shall be responsible for any loss, harm, damage, and expense which may be suffered by you or any third-party, which may be attributable to your access and use of the Website, or any information contained on or received via the Website.

The Indemnified Parties shall not be liable for any loss of business, data or profits, failure, or unavailability of the Website for any reason, and failure by any third-party service provider to render any service which are necessary to ensure the availability of the Website.

You hereby indemnify the Indemnified Parties against any loss, liability, harm, damage, or expense which may be suffered by you or any third-party because of or which may be attributable to any of the above.

2.4.9. INDEMNITY

In addition to the warranties and indemnities set out above, you hereby agree to hold harmless the Indemnified Parties from any claims, damages, obligations, losses, liabilities, costs or debt, and expenses arising from:

- Your violation of any provision of these terms.
- Your violation of any third party right including any Intellectual Property Right, or other property or privacy right.
- Any claim that the user content caused damage to a third-party.

2.4.10. EXTERNAL LINKS

External links may be provided for your convenience; however, the Company makes no representations whatsoever about any third-party Website or its content. Use of any external links provided is entirely at your own risk. It is your responsibility to ensure that you obtain all relevant information and that you read the privacy and security policy displayed on any third-party Website. The Company has no control over such third-party websites and will not be liable for any loss or damage that you may suffer, because of your use of third-party websites.

2.4.11. GOVERNING LAW

These Terms shall be governed in accordance with the laws of the Republic of South Africa, and you hereby submit to the jurisdiction of the South African courts. If any provision of these Terms is found to be unlawful, void, or for any reason unenforceable by a competent court in the Republic of South Africa, then that provision shall be severable from these Terms and shall not affect the validity and enforceability of any remaining provisions.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

SECTION 3: DATA MANAGEMENT SYSTEM

3.1. General Notice

3.1.1. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

3.1.2. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

3.1.3. POLICY AWARENESS AND UPDATE

Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.2. Policy: Information Security Management

3.2.1. PURPOSE

All organisations that process any information that identifies an individual or juristic entity, must implement information security measures. Information security measures mean the processes that are implemented by the Company to protect printed, electronic, and any other form of sensitive or confidential information, and personal information from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

This Policy regulates the information security measures implemented by the Company. Where the information being processed consists of personal information, the provisions of the Protection of Personal Information Act 4 of 2013 (POPIA) will apply.

The purpose of this Policy is to ensure:

- The provision of reliable and uninterrupted Information Systems.
- The integrity and validity of data contained in Information Systems.
- An ability to recover effectively and efficiently from disruption to Information Systems.
- The protection of the Company's Information Technology assets including information, software, and hardware.

Within this Policy, information assets (e.g., databases, files), software assets (e.g., applications and systems software and development tools), and hardware assets (e.g., computers, communications equipment, and magnetic media) refer to those assets which taken together comprise the Company's Information Systems.

Please refer to Annexure A for a list of all Company Devices.
Please refer to Annexure B for a list of all Company Software.

3.2.2. OBJECTIVE

The objective of this Policy is to:

- Regulate the information security environment of the Company.
- Set out the responsibilities of persons in the information security environment.
- Improving information security in the Company.

It is important to ensure that information security measures address the confidentiality, integrity, and availability of information.

This Policy applies to all employees, contractors, visitors, and other persons authorised to access and use the Company's systems, that create and use records that relate to the Company's business operations.

3.2.3. POLICY

The Company will apply the measures necessary to ensure the confidentiality, integrity and availability of confidential information, and personal information. The Company will identify personal information and ensure that the information is protected in accordance with the requirements required by POPIA.

Please refer to Annexure D: List of personal information collected by the company.

Please refer to Annexure E: Categorise the personal information collected by the company.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Please refer to Annexure F: Reason for the personal information collected by the company.

Where the Personal Information in question is more sensitive in nature, such as information pertaining to minors, health and sex life, the Company will ensure that more stringent measures required under POPIA, are implemented.

3.2.4. PERSONAL INFORMATION NEEDING PROTECTION IN TERMS OF POPIA

(Section 1 of the Protection of Personal Information Act 4 of 2013)

PERSONAL INFORMATION NEEDING PROTECTION		
SECTION 1 PERSONAL INFORMATION	**DESCRIPTION**	**EXAMPLE**
SECTION 1(a)	Information relating to the 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.	Information often found in records of businesses, e.g., HR Records, hospital records, consumer records, supplier Records.
SECTION 1(b)	Information relating to the education or the medical, financial, criminal or employment history of the person.	Information often found in records of universities, hospitals, banks and insurance companies, police and HR records of companies, supplier records held by companies, consumer records, supplier records, held by companies. Such as bank details and invoices. CVs of job applicants.
SECTION 1(c)	Any identifying number, symbol, email address, physical address, telephone number, location Information, online identifier, or other particular assignment to the person.	I.D. Number, GPS location, IP address, Employee number.
SECTION 1(d)	The blood type or any other biometric Information of the person.	Blood type, DNA., fingerprints, CCTV footage.
SECTION 1(e)	The personal opinions, views, or preferences of the person.	Feedback reports, staff performance reviews, emails.

SECTION 1(f)	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.	Doctor's letter, email, WhatsApp messages, handwritten notes.
SECTION 1(g)	The views or opinions of another individual about the person.	Performance review, emails, notes, messages.
SECTION 1(h)	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.	Name and address, business name and registration number, email address, contacts on mobile phone.

3.2.5. THE 8 CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

1. **Accountability (POPIA Section 8)**

As a Company, everything reasonably within the Company's power must be done, to ensure that the conditions of POPIA have been properly complied with by employees and business partners.

2. **Processing Limitation (POPIA Sections 9 - 12)**

Information must be processed within the parameters of the law, and only that which is necessary to fulfil the Company's business practices may be used. The Company must obey the rule of consent and have measures in place to action any objections it might face, from data subjects.

3. **Purpose specification (POPIA Sections 13 - 14)**

Information is only collected and used for carefully defined purposes. Care should be taken to specify these purposes at points of collection. Information held by the Company should be held for minimal periods, ensuring that data is never retained for longer than is necessary to fulfil business practices or obligations to the law (*Refer to Data Retention and Destruction Policy*).

4. **Further processing limitation (POPIA Section 15)**

Information that is stored, is only reused if this usage aligns with the purpose for which the Information was collected. Consent must be revisited at all instances where change is necessary.

5. **Information quality (POPIA Section 16)**

Information usage must be guided by 'quality over quantity' and therefore the Company needs to ensure that the information it manages is complete, accurate, not misleading in nature and updated.

6. **Openness (POPIA Sections 17, 18, 57, 58(1)(2))**

The Company should be compliant with complementary laws such as the Promotion of Access to Information Act of 2002 (PAIA) and have a process in place to provide access to Information for those requiring it. The Company should ensure that no information is collected unless the data subject fully

understands the implications of sharing their information, and whom to contact if they are dissatisfied with Information security.

7. Security safeguards (POPIA Sections 19 - 22)

The Company should conform to industry standards related to securing the information which they hold and be committed to only contract with other businesses who do the same. The Company should ensure that its security systems and contingency plans are in place for breaches of security, and these should be tested at regular intervals.

8. Data subject participation (POPIA Sections 22 - 24)

Data subjects have a right to know when their Information is being collected and what exactly is being stored. The Company should have measures in place to answer questions which their data subjects may have, about their information. The data subjects should be empowered to make corrections or request removals where necessary.

3.2.6. RESPONSIBILITIES IN RELATION TO INFORMATION SECURITY

The various responsibilities in terms of this Policy must be implemented throughout the Company.

Information Systems hosted off-site must comply with the Company's guidelines.

The Company accepts that cyber-security risks are a reality, and the data-breaches may occur, despite the reasonable measures undertaken by the Company. Should such a breach occur, it is the responsibility of the Company to:

- Notify the Information Regulator within 72 hours from detection of the breach.
- Notify data subjects within 72 hours of the detection of the breach.
- Carry the costs of these notifications.
- Act on all Notices of Non-Compliance or Notices of Investigation from the Information Regulator.
- Carry the legal costs for the Company during these investigations.

3.2.7. RISK ASSESSMENT

The Company will carry out regular risk assessments of its Information Systems. These risk assessments will examine potential vulnerabilities and will lead to the development of controls consistent with minimising the identified risk to an acceptable level.

3.2.8. ACCESS MANAGEMENT

All users must be authorised to access the Company's Information Systems. Access is controlled and monitored in accordance with the Company's Access to Personal Information Policy.

Authorisation:
Only those users who have valid reasons for accessing the Company's Information Systems are granted access privileges appropriate to their requirements.

Authentication:
Authentication ensures an identity. Each authentication requires a technique, usually a password, for validating identity.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Privileged Users:
System administrators have high-level access rights, enabling them to access any data stored on the Company's Information Systems. System administrators should abide by the applicable Acceptable Usage Policy and should sign a Confidentiality Agreement (*Refer to Annexure C for the Employee Confidentiality Agreement*).

System Administrators found guilty of breaching the *Acceptable Usage Policy* may be subject to disciplinary action as recommended by the Information Officer.

Contractor and third-party access are permitted only if agreed to by the Information Officer. These parties must comply with access control standards.

3.2.9. INFORMATION ASSET SECURITY MANAGEMENT SUMMARY

All major Information Systems must have a nominated owner who is responsible for the implementation and management of this Policy in relation to those assets.

Please refer to Annexure A for a list of all Company Devices.
Please refer to Annexure B for a list of all Company Software.

Server and System Backup	All Personal Information held by the Company should be stored on maintained networked disc storage and must be backed up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the Information if lost. Data stored in other locations, e.g., on servers, desktops, laptops, and other mobile devices becomes the responsibility of the user to ensure it is backed up on a regular basis (*Refer to Backup and Restoration Policy*).
Recovery	All backups of critical data must be tested periodically to ensure that they support full system recovery. System Administrators must test these on a regular basis. Backup media must be retrievable within 24 hours, 365 days a year.
Off-Site Storage (Backup Media)	Off-site storage locations must provide evidence of adequate fire and theft protection and environmental controls. A formal Service Level Agreement (SLA), DPA or GDPR agreement must exist with the off-site storage provider (*Refer to Data Operator Policy*).
Data Retention	The Company is responsible for documenting the length of time data must be retained. The retention period, legal requirements and source of legal requirement should be specified. *(Refer to the Data Retention and Destruction Policy)*
Business Continuity and Disaster Recovery	The testing strategy must be implemented. It will be influenced by the importance of the system to the Company's business operations and the ability to recover the system within agreed timeframes.
Physical Security	Access to secure areas, including computer rooms, network equipment rooms and any associated service facilities, is restricted to authorised Company's personnel (*Refer to Record Access Control Policy*).

Software Security	Software for the purpose of this Policy is defined as the programmes and other operating information used by, installed on, or stored on the Company owned computer systems or storage media. System Administrators must ensure that software is licensed in an appropriate manner. All software, including patches, upgrades, or new versions, should be tested, archived, and documented before being put into production.
Internet Security	Computer devices connected to the Internet face significant risk of unauthorised access or inappropriate use. Several measures should be taken to mitigate this risk (*Refer to Acceptable Usage Policy*).
Email Security	Unsolicited e-mail can affect the performance of the e-mail delivery system and the productivity of the user. To reduce the level of unsolicited messages, e-mail that meets one or more of the following criteria must be blocked or rejected: • Malformed e-mail. • E-mail with an attachment identified as a significant risk. • E-mail that exhibits a significant level of unsolicited e-mail characteristics.

3.2.10. INFORMATION CLASSIFICATION

Information is classified into four categories: Public, Internal, Confidential and Restricted.

Public	Public Information can generally be made available or distributed to the public. This is information which does not require protection and when used would have little to no adverse effect on the operations, assets, or reputation of the Company.
Internal	Internal Information is for general internal business use only and not for external distribution. Internal Information may be accessed by authorised personnel at the Company.
Confidential	Confidential Information is for internal use only with access only by employees who require it while performing their responsibilities. Confidential Information includes information that is protected by legislation or business contractual obligations and requires privacy and security protections.
Restricted	Restricted Information is to be kept strictly confidential with access on a need-to-know basis. This includes Personal Information and Special Personal Information

Employees should be aware of their legal responsibilities concerning inappropriate use, sharing, or releasing of information to another party. Any third-party receiving Confidential or Restricted Information must have adopted information security measures, which guarantee confidentiality and integrity of that data.

Refer to Annexure D for Type of Personal Information Collected
Refer to Annexure E for Classification of Personal Information

3.2.11. HANDLING AND DISTRIBUTION OF INFORMATION ASSETS

The following restrictions apply to the handling of Information assets.

Public Information.

Description	There are no specific restrictions on the distribution or handling of public Information, although the Company's personnel must respect all copyright, trademark and intellectual property rights of any information or data that they distribute.
Access	n/a
Distribution within the Company	n/a
Distribution outside the Company	n/a
Storage	n/a
Disposal / Destruction	n/a

Internal Information

Description	Internal Information is considered non-public and should be protected from unnecessary exposure to parties outside of the Company.
Access	The Company's employees, or non-employees with signed Non-Disclosure Agreements (NDA), who have a legitimate business need to know. *(Refer to Data Operator Policy)*
Distribution within the Company	Information can be shared via the web. Electronic and hard copy Information can be circulated on a need-to-know basis within the Company. Internal information may be accessed remotely and via disk-encrypted portable and mobile devices without further encryption.
Distribution outside the Company	Information can be sent in unencrypted format via the Company's e-mail to external parties on a need-to-know basis. Information can be shared using the Company's IT facilities, e.g., OneDrive, Dropbox, or shared file servers. Information can be circulated via the Company's internal e-mail system.
Storage	Must be stored using the Company's provided facilities
Disposal / Destruction	Electronic data should be securely and reliably erased, or media physically destroyed.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Confidential Information

Description	Confidential Information should be protected to prevent unauthorised access or exposure.
Access	The Company's employees whose job function requires them to have access, and the Company's suppliers or consultants who have executed Non-Disclosure Agreements (NDA) with the Company. *(Refer to Data Operator Control Policy)*
Distribution within the Company	Access to confidential data must be strictly controlled. Confidential Information may be shared with authorised users via the Company's IT facilities, including remote access, subject to the Company's authentication. Encryption of data must be used for all web-based access to Confidential Information. Confidential data must not be extracted from the Company's IT systems. If a portable device is used to access the Company's Confidential Information, the device must be encrypted and require a password or PIN to access.
Distribution outside the Company	Electronic files must be encrypted or be password protected at the application level. The encrypted / password-protected files can then be sent via e-mail or secure electronic file transmission. Third-parties who are handling and storing Confidential Information must agree to abide by the Company's Policies for safeguarding such Information *(Refer to Data Operator Control Policy).*
Storage	Information must be stored using the Company's IT facilities. Portable devices must have full disk encryption. Unencrypted removable media (e.g., USB sticks or drives) must not be used. Encrypted removable media are not permitted. Storage on personally owned computer is not permitted. *(Refer to Acceptable Usage Policy)*.
Disposal / Destruction	Confidential Information should be protected to prevent unauthorised access or exposure.

Restricted Information

Description	Restricted Information has the highest level of sensitivity and represents the most risk to the Company and individuals should such Information be accessed by or exposed to unauthorised parties. The Company's employees who handle Restricted Information or who use systems that store, transmit, or manipulate Restricted Information are required to maintain the confidentiality, integrity, and availability of such Information always.
Access	The access, distribution, storage, and disposal of Restricted Information may be subject to applicable legislation and will require approval and review of the Information Officer.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Distribution within the Company	Access to Restricted Information must be strictly controlled. Restricted Information may be shared with authorised users via the Company's IT facilities, subject to the Company's authentication. Encryption of data must be used for all web-based access to Restricted Information. Restricted data must not be extracted from the Company's IT systems. If a portable device is used to access the Company's Restricted Information, the device must be encrypted and require a password or PIN to access.
Distribution outside the Company	Electronic files must be encrypted or be password protected at the application level. The encrypted/ password-protected files can then be sent via e-mail or secure electronic file transmission. Third Parties who are handling and storing Restricted Information must agree to abide by the Company's Policies for safeguarding such Information *(Refer to Data Operator Control Policy)*.
Storage	Information must be stored using the Company's IT facilities. Portable devices must have full disk encryption. Unencrypted removable media (e.g., USB sticks or drives) must not be used. Encrypted removable media are not permitted. Storage on Personally owned computer is not permitted *(Refer to Acceptable Usage Policy)*.
Disposal / Destruction	Restricted Information should be protected to prevent unauthorised access or exposure.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (3.2) D: LIST OF PERSONAL INFORMATION COLLECTED BY THE COMPANY

Please think carefully about what data the Company collects from businesses, individuals, and employees. Mark the appropriate block.

There are four categories of data collection: Individuals, Children, Businesses and Employees. Tick the appropriate block if the Company collects information on a certain category. If the Company collect information of individuals within a business, please tick the Individual box as well.

(Please note that the Individual Category covers both living and deceased individuals)

Information Type	Category			
Name & Surname / Business name	Individuals	Businesses	Children	Employees
Email	Individuals	Businesses	Children	Employees
Contact Information	Individuals	Businesses	Children	Employees
Physical / Postal Address	Individuals	Businesses	Children	Employees
Income (Earned and Unearned)	Individuals	Businesses	Children	Employees
Banking Details	Individuals	Businesses	Children	Employees
Annual Income / Turnover	Individuals	Businesses	Children	Employees
Date of Birth	Individuals	Businesses	Children	Employees
Nationality	Individuals	n/a	Children	Employees
Gender	Individuals	n/a	Children	Employees
Ethnicity	Individuals	n/a	Children	Employees
Religion	Individuals	n/a	Children	Employees
Language	Individuals	n/a	Children	Employees
Record of working time	Individuals	n/a	n/a	Employees
Tax Data	Individuals	Businesses	Children	Employees
Photographs	Individuals	Businesses	Children	Employees
Race	Individuals	n/a	Children	Employees
Pregnancy	Individuals	n/a	Children	Employees

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Age	Individuals	n/a	Children	Employees
Marital Status	Individuals	n/a	Children	Employees
Physical Health	Individuals	n/a	Children	Employees
Mental health	Individuals	n/a	Children	Employees
Conscience	Individuals	n/a	Children	Employees
Disability	Individuals	n/a	Children	Employees
Belief	Individuals	n/a	Children	Employees
Culture	Individuals	n/a	Children	Employees
Education	Individuals	n/a	Children	Employees
Medical Information	Individuals	n/a	Children	Employees
Financial Information	Individuals	Businesses	Children	Employees
Criminal Information	Individuals	Businesses	Children	Employees
Identity Numbers	Individuals	Businesses	Children	Employees
Legal Information	Individuals	Businesses	Children	Employees
Employment History	Individuals	Businesses	Children	Employees
Biometric Information	Individuals	Businesses	Children	Employees
Personal Opinions / Views	Individuals	Businesses	Children	Employees
Correspondence (Emails, Letters, or notes)	Individuals	Businesses	Children	Employees
Credit References	Individuals	Businesses	Children	Employees
Next of Kin	Individuals	Businesses	Children	Employees
Trade Union membership	Individuals	Businesses	n/a	Employees
Political Persuasion	Individuals	Businesses	Children	Employees
Health or Sex life	Individuals	n/a	Children	Employees
Criminal Behaviour	Individuals	Businesses	Children	Employees
Performance Reviews	Individuals	Businesses	Children	Employees

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Legal Proceedings	Individuals	Businesses	Children	Employees
CV's	Individuals	n/a	Children	Employees
Employment History	Individuals	Businesses	n/a	Employees
IP addresses	Individuals	Businesses	Children	Employees
Genetic Information	Individuals	n/a	Children	Employees
Information on payments	Individuals	Businesses	Children	Employees
Video Surveillance /CCTV	Individuals	Businesses	Children	Employees
Fingerprints	Individuals	n/a	Children	Employees

Specify any other Personal Information that the Company collects:

Information Type	**Category**			
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees
	Individuals	Businesses	Children	Employees

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (3.2) E: CATEGORISE THE PERSONAL INFORMATION COLLECTED BY THE COMPANY

Please think carefully about what data the Company collects from businesses, individuals, and employees. Mark the appropriate block.

There are four categories of data categorisation: Public, Internal, Confidential and Restricted. Tick the appropriate block.

(Please note that the Individual Category covers both living individuals, deceased individuals, as well as juristic entities)

Information Type	Category			
Name & Surname / Business name	Public	Internal	Confidential	Restricted
Email	Public	Internal	Confidential	Restricted
Contact Information	Public	Internal	Confidential	Restricted
Physical / Postal Address	Public	Internal	Confidential	Restricted
Income (Earned and Unearned)	Public	Internal	Confidential	Restricted
Banking Details	Public	Internal	Confidential	Restricted
Annual Income / Turnover	Public	Internal	Confidential	Restricted
Date of Birth	Public	Internal	Confidential	Restricted
Nationality	Public	Internal	Confidential	Restricted
Gender	Public	Internal	Confidential	Restricted
Ethnicity	Public	Internal	Confidential	Restricted
Religion	Public	Internal	Confidential	Restricted
Language	Public	Internal	Confidential	Restricted
Record of working time	Public	Internal	Confidential	Restricted
Tax Data	Public	Internal	Confidential	Restricted
Photographs	Public	Internal	Confidential	Restricted
Race	Public	Internal	Confidential	Restricted
Pregnancy	Public	Internal	Confidential	Restricted

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Age	Public	Internal	Confidential	Restricted
Marital Status	Public	Internal	Confidential	Restricted
Physical Health	Public	Internal	Confidential	Restricted
Mental health	Public	Internal	Confidential	Restricted
Conscience	Public	Internal	Confidential	Restricted
Disability	Public	Internal	Confidential	Restricted
Belief	Public	Internal	Confidential	Restricted
Culture	Public	Internal	Confidential	Restricted
Education	Public	Internal	Confidential	Restricted
Medical Information	Public	Internal	Confidential	Restricted
Financial Information	Public	Internal	Confidential	Restricted
Criminal Information	Public	Internal	Confidential	Restricted
Identity Numbers	Public	Internal	Confidential	Restricted
Legal Information	Public	Internal	Confidential	Restricted
Employment History	Public	Internal	Confidential	Restricted
Biometric Information	Public	Internal	Confidential	Restricted
Personal Opinions / Views	Public	Internal	Confidential	Restricted
Correspondence (Emails, Letters, or notes)	Public	Internal	Confidential	Restricted
Credit References	Public	Internal	Confidential	Restricted
Next of Kin	Public	Internal	Confidential	Restricted
Trade Union membership	Public	Internal	Confidential	Restricted
Political Persuasion	Public	Internal	Confidential	Restricted
Health or Sex life	Public	Internal	Confidential	Restricted
Criminal Behaviour	Public	Internal	Confidential	Restricted
Performance Reviews	Public	Internal	Confidential	Restricted

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Legal Proceedings	Public	Internal	Confidential	Restricted
CV's	Public	Internal	Confidential	Restricted
Employment History	Public	Internal	Confidential	Restricted
IP addresses	Public	Internal	Confidential	Restricted
Genetic Information	Public	Internal	Confidential	Restricted
Information on payments	Public	Internal	Confidential	Restricted
Video Surveillance /CCTV	Public	Internal	Confidential	Restricted
Fingerprints	Public	Internal	Confidential	Restricted

Categorise any other Personal Information that the Company collects.

Information Type	**Category**			
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted
	Public	Internal	Confidential	Restricted

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (3.2) F: REASON FOR THE COLLECTION OF PERSONAL INFORMATION BY THE COMPANY

Please think carefully about why the Company collects data from businesses, individuals, and employees. Mark the appropriate block.

There are different reasons of data collection:

- *Marketing: This includes emails, phone calls, SMS, newsletters, promotions, or any other type of marketing.*
- *Internal Business Function: This includes HR functions, payroll, employee contracts and files, occupational health and safety, SARS, or any other internal business function.*
- *Business Transaction: This includes payments, banking, invoicing, proof of payments, or any other financial transaction.*
- *Data Operators: This includes details about any of your service providers, distributers, suppliers, external data processors or any other external business function with a third-party.*
- *If the Company collects personal or special personal information for any other reason, please specify in the Other block.*

Tick the appropriate block.

(Please note that the data collection includes both living individuals, deceased individuals, as well as juristic entities)

Information Type	**Category**				
	Marketing	**Internal Business Function**	**Business Transactions**	**Data Operators**	**Other: Specify**
Name & Surname / Business name	Marketing	Internal Business Function	Business Transactions	Data Operators	
Email	Marketing	Internal Business Function	Business Transactions	Data Operators	
Contact Information	Marketing	Internal Business Function	Business Transactions	Data Operators	
Physical / Postal Address	Marketing	Internal Business Function	Business Transactions	Data Operators	
Income (Earned and Unearned)	Marketing	Internal Business Function	Business Transactions	Data Operators	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Banking Details	Marketing	Internal Business Function	Business Transactions	Data Operators	
Annual Income / Turnover	Marketing	Internal Business Function	Business Transactions	Data Operators	
Date of Birth	Marketing	Internal Business Function	Business Transactions	Data Operators	
Nationality	Marketing	Internal Business Function	Business Transactions	Data Operators	
Gender	Marketing	Internal Business Function	Business Transactions	Data Operators	
Ethnicity	Marketing	Internal Business Function	Business Transactions	Data Operators	
Religion	Marketing	Internal Business Function	Business Transactions	Data Operators	
Language	Marketing	Internal Business Function	Business Transactions	Data Operators	
Record of working time	Marketing	Internal Business Function	Business Transactions	Data Operators	
Tax Data	Marketing	Internal Business Function	Business Transactions	Data Operators	
Photographs	Marketing	Internal Business Function	Business Transactions	Data Operators	
Race	Marketing	Internal Business Function	Business Transactions	Data Operators	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Pregnancy	Marketing	Internal Business Function	Business Transactions	Data Operators	
Age	Marketing	Internal Business Function	Business Transactions	Data Operators	
Marital Status	Marketing	Internal Business Function	Business Transactions	Data Operators	
Physical Health	Marketing	Internal Business Function	Business Transactions	Data Operators	
Mental health	Marketing	Internal Business Function	Business Transactions	Data Operators	
Conscience	Marketing	Internal Business Function	Business Transactions	Data Operators	
Disability	Marketing	Internal Business Function	Business Transactions	Data Operators	
Belief	Marketing	Internal Business Function	Business Transactions	Data Operators	
Culture	Marketing	Internal Business Function	Business Transactions	Data Operators	
Education	Marketing	Internal Business Function	Business Transactions	Data Operators	
Medical Information	Marketing	Internal Business Function	Business Transactions	Data Operators	
Financial Information	Marketing	Internal Business Function	Business Transactions	Data Operators	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Criminal Information	Marketing	Internal Business Function	Business Transactions	Data Operators	
Identity Numbers	Marketing	Internal Business Function	Business Transactions	Data Operators	
Legal Information	Marketing	Internal Business Function	Business Transactions	Data Operators	
Employment History	Marketing	Internal Business Function	Business Transactions	Data Operators	
Biometric Information	Marketing	Internal Business Function	Business Transactions	Data Operators	
Personal Opinions / Views	Marketing	Internal Business Function	Business Transactions	Data Operators	
Correspondence (Emails, Letters, or notes)	Marketing	Internal Business Function	Business Transactions	Data Operators	
Credit References	Marketing	Internal Business Function	Business Transactions	Data Operators	
Next of Kin	Marketing	Internal Business Function	Business Transactions	Data Operators	
Trade Union membership	Marketing	Internal Business Function	Business Transactions	Data Operators	
Political Persuasion	Marketing	Internal Business Function	Business Transactions	Data Operators	
Health or Sex life	Marketing	Internal Business Function	Business Transactions	Data Operators	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Criminal Behaviour	Marketing	Internal Business Function	Business Transactions	Data Operators	
Performance Reviews	Marketing	Internal Business Function	Business Transactions	Data Operators	
Legal Proceedings	Marketing	Internal Business Function	Business Transactions	Data Operators	
CV's	Marketing	Internal Business Function	Business Transactions	Data Operators	
Employment History	Marketing	Internal Business Function	Business Transactions	Data Operators	
IP addresses	Marketing	Internal Business Function	Business Transactions	Data Operators	
Genetic Information	Marketing	Internal Business Function	Business Transactions	Data Operators	
Information on payments	Marketing	Internal Business Function	Business Transactions	Data Operators	
Video Surveillance /CCTV	Marketing	Internal Business Function	Business Transactions	Data Operators	
Fingerprints	Marketing	Internal Business Function	Business Transactions	Data Operators	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Categorise any other Personal Information that the Company collects.

Information Type	**Category**				
	Marketing	**Internal Business Function**	**Business Transactions**	**Data Operators**	**Other: Specify**
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	
	Marketing	Internal Business Function	Business Transactions	Data Operators	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.3. Policy: Acceptable Usage Policy

3.3.1. PURPOSE

This Policy should be given to every User before they commence work utilising Company resources.

To remain competitive, better serve the consumer and provide employees with the best tools to do their jobs, the Company makes available to our workforce access to one or more forms of electronic media and services, including computers, e-mail, telephones, external electronic bulletin boards, wire services, online services, intranet, Internet, mobile phones, tablets, laptops, and the World Wide Web.

The Company encourages the use of these media and associated services because they can make communication more efficient and effective. Also, they are valuable sources of information about vendors, customers, technology, and new products and services. However, all employees and everyone connected with the Company (Users) should remember that electronic media and services provided by the Company are Company property and their purpose is to facilitate and support Company business. All computer Users have the responsibility to use these resources in a professional, ethical, and lawful manner.

This Acceptable Usage Policy states what information Users authorised to access and use the Company's systems, are and are not permitted to use. It is important to apply information security principles to protect the confidentiality, integrity, and availability of information. Without this Policy, Users could violate information security and avoid disciplinary actions by claiming not to be aware about any restrictions that the Company set out. So that all Users are responsible and accountable, the following guidelines have been established for using Company Resources.

3.3.2. SCOPE

This Policy applies to all Users (employees and third-parties) of all information systems that belong to the Company.

This Policy must be read in conjunction with the *Personal Information of Employees Policy*.

3.3.3. POLICY

The Company will issue various acceptable usage guidelines in this Policy covering the following items:

- Computer and information technology system usage.
- Software and data usage.
- Internet and email usage.
- Newsgroups.
- Social Media platforms
- Telephone usage.
- Office equipment and materials usage.
- Social media usage.
- Participation in online forums
- Video conferencing.
- Mobile devices
- Password protocols
- IT security.
- Privacy and confidentiality.

3.3.4. USAGE GUIDELINES

Users must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorisation has been granted by Company management, Users are prohibited from engaging in:

- Monitoring or intercepting the files or electronic communications of other Users.
- Hacking or obtaining access to systems or accounts they are not authorised to use.
- Using other people's login details or passwords.
- Breaching, testing, or monitoring computer or network security measures.

No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else. Electronic media and services should not be used in a manner that is likely to cause network congestion or hamper the ability of other people to access and use the system. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights.

3.3.5. COMPUTER AND IT SYSTEM USAGE

Systems, including computers and other related technology, are the property of the Company. Access to, and use of, Company systems and their components will be monitored and controlled.

Compliance with this Policy is an effort that requires Users to act responsibly and guard against abuse. Therefore, each User has an obligation to abide by the following standards of acceptable and ethical use. The following conduct is not permitted:

- Accessing computers, computer software, computer data or information, or networks without proper authorisation, regardless of whether the Company owns the computer, software, data, information, or network in question.
- Transmitting on or through any of the Companies systems, services, or products any material that is unlawful, obscene, racial, pornographic, threatening, abusive, libellous, or hateful, or encourages conduct that may constitute a criminal offence.
- Consuming excessive resources, including central processing unit time, memory, disk space and the like, and all session time for personal use, is prohibited.
- Intercepting or examining the content of messages or files in transit on a network without authorisation from the owner of the information.

3.3.6. SOFTWARE AND DATA USAGE

The software tools of the Company, and the data they collect, create and process, belong to the Company. Software is to be used for its intended purpose only. It is not to be copied, reverse-engineered, distributed, installed, or deleted without appropriate authorisation.

Violating any software license agreement or intellectual property right, including copying, adapting, or redistributing copyrighted software, data, or reports without proper, recorded authorisation, is prohibited. Violating the intellectual property rights of software holders, or the holders of computer-generated data or reports, without proper, recorded authorisation, is prohibited.

3.3.7. INTERNET AND EMAIL USAGE

It is a violation of this Policy to send email that contain personal identifiable information as described in POPIA, without considering the appropriate protection required in relation to such emails. Emails of this nature must at the very least be password protected.

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing.
2. Derogatory to any individual or group.

3. Obscene, sexually explicit, or pornographic.
4. Defamatory or threatening.
5. Harmful to morale.
6. Creating or forwarding pyramid schemes of any type, whether the recipient wishes to receive such mailings or not, is prohibited.
7. Forbidden transmissions, which includes but is not limited to:
    - Sexually explicit messages.
    - Unwelcome propositions of love letters.
    - Ethnic or racial slurs.
    - Or any other message that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, or religious or political beliefs.
    - No abusive, profane, or offensive language is to be transmitted through the company's e-mail or Internet system.
    - Electronic media may also not be used for any other purpose which is illegal, or against Company policy or contrary to the Company's best interest.
8. Engaged in for any purpose that is illegal or contrary to Company policy or business interests.
9. Malicious email including, flooding a User or site with large or numerous pieces of email is prohibited.
10. It is a violation of this Policy to forge an email signature to make it appear as though it originated from a different person.
11. It is a violation of this Policy to use a Company or a client account to collect replies to messages sent from another party.
12. It is a violation of this Policy to attempt to gain access to another person's email files.
13. It is a violation of this Policy to send unauthorised copyrighted materials electronically.
14. All Users are required to keep all login details, including username and passwords, confidential and may not share these details with any other person.
15. Users whose employment or other relationship with the Company has been terminated will have no rights of access to the contents of messages addressed to them, whether in an official or private capacity.

While some Users include personal disclaimers in electronic messages, there is still a connection to the Company, and the statements may be tied to the Company.

Internet and email usage must be restricted, as both activities make use of public and unsecured networks. The Internet is to be used for business purposes only and usage will always be monitored and controlled by the Company. Causing security breaches or disruptions of internet communications is strictly prohibited. Security breaches include, accessing data not intended for the User in question, or logging onto a server or account that the User is not expressly authorised to access.

When reference is made to, "disruption", it shall include, port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, attempts to crash a host, and the introduction of any malicious code, such as computer viruses or "trojans", onto any part of the Company's computer network.

Users should be aware of the risks of using emails and how they may inadvertently disclose personal information. Users should be alert to new scams around phishing, social engineering, man-in-the-middle attacks, etc. The following email protocols will be implemented to comply to POPIA regulations in the Company:

- Users are only to use work-related email accounts for work-related purposes.
- If processing Personal Information through work email accounts, ensure that the files are encrypted.
- Avoid using Personal Information in subject lines.
- Ensure that emails are sent to the correct recipients, particularly emails involving Personal Information.

- Do not use the “Reply All’ button before considering if it is necessary for all the recipients to see the content of your email, and if they are authorised to do so.
- Be aware of long email strings and threads, created by “Forwarding” or “Replying” to emails, without having checked if all the information is permitted to be disclosed to the recipient of your email. It often happens that confidential internal correspondence is inadvertently disclosed to third-parties or clients in this manner.
- Do not disclose the email addresses of a group of recipients in a visible manner, unless you have their explicit consent to do so. The use of the “CC” function is prohibited.
- All employees must include the following Email Disclaimer as part of their email:

“*Please do not print this email unless it is necessary. Every unprinted email helps the environment.*

The information contained in this electronic message is confidential. It is intended solely for the use of the receiver to whom the Company has addressed the electronic message and others expressly authorised by the Company. If you are not the intended receiver, you are hereby notified that any disclosure, copying, distribution or acting in reliance of the contents of this information is strictly prohibited and may be unlawful. The Company is not liable for any harm or loss resulting from malicious software code or viruses in this e-mail or its attachments, including data corruption resulting there from. Any advice or information contained in this e-mail is subject also to any governing agreement between us. No electronic communication including any data message such as an e-mail or SMS, sent or received will give rise to a binding legal transaction. The Company respects your privacy and acknowledge that this e-mail will contain personal details, which may belong to you, others and/or to your company (Personal Information). By sending the Company this email communication, you expressly give the Company consent to process and further process the Personal Information which will be done in accordance with the Protection of Personal Information Act (4 of 2013) (POPIA). “

3.3.8. NEWSGROUPS

The following serves as a guideline as to what the Company considers the misuse of computing resources and privileges. These actions are prohibited except when the User is authorised to do so by the Company as part of normal business practice and their specific function within the Company:

- Posting the same or similar messages to large numbers of newsgroups (known as newsgroup or USENET spam).
- Posting encoded binary files to newsgroups not specifically named for that purpose.
- Cancellation or superseding of posts other than a User’s own posts, except for official newsgroup moderators performing their duties.
- Forging of header information, which includes the circumvention of the approval process for posting to a moderated newsgroup.
- Solicitation of email from any other email address other than the User’s account or service, with the intent to harass or collect replies.
- Posting of articles from the Company network on behalf of, or to advertise any service provided by the Company or connecting via the Company’s network without written permission from the Company.

3.3.9. TELEPHONE USAGE

Telephone usage guidelines (this includes land-lines and mobile phones belonging to the Company):

- Telephones should be used in a courteous and professional manner.

- Users using the telephone for private use may be required to reimburse the Company.
- In addition to the above, the Company reserves the right to take disciplinary action against any User who misuses the company telephone system.
- Any person who uses the Company telephones for what could be terms as unsuitable uses will be subject to a formal enquiry.
- The unsuitable uses include but are not limited to:
    - Contact with adult phone lines or emails of a graphic, pornographic, or adult content.
    - Using company telephones to conduct private business.
    - Receiving of email or social media messages, which may be deemed as unsuitable to the public.

This policy is applicable to all Company equipment and should not be perceived as only relating to telephone usage. The utilisation of all Company equipment, services and facilities will be monitored on a regular and on-going basis. Unauthorised use of any equipment and facilities shall be subject to disciplinary action. The Company will not be liable in any way because of any communication or information that may be deemed to be offensive. All rights are reserved in this regard.

3.3.10. OFFICE EQUIPMENT AND MATERIALS USAGE

All office materials, furnishings and supplies provided to Users are the property of the Company and are to be used for business purposes only. Generic materials, such as pens, blank paper, and the like, may be freely accessed but are not to be removed from the Company without the prior consent of the Company.

Specific materials such as letterheads must and will have restricted access and are not to be removed from the Company premises without the prior consent of the Company. Users are not permitted to place any Company material, including software or internal memos, on any publicly accessible internal or external website without the prior approval of the Company.

3.3.11. SOCIAL MEDIA USAGE

The Company's social media accounts are intended to be used, solely for business purposes. The following activities are deemed to be inappropriate use of social media:

- Use of social media for illegal or unlawful purposes, including copyright infringement, obscenity, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering including, spreading of computer viruses.
- Use of social media that in any way violates the Company's policies, rules or administrative orders that may be applicable.
- Opening attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with the utmost caution.
- Sharing social media account passwords with another person or attempting to obtain another person's social media account password.

3.3.12. PARTICIPATION IN ONLINE FORUMS

Users should remember that any messages or information sent on company-provided facilities to one or more individuals via an electronic network, for example, Internet mailing lists, bulletin boards, and online services, are statements identifiable and attributable to the Company.

3.3.13. VIDEO CONFERENCING

The use of video conferring is for business purposes only and the following conditions must be adhered to:

- Users are required to always act professionally and respectfully.
- Video conferences are required to be treated like a normal meeting with a client.
- No foul language should be used.
- If a User's screen is being shared, such User is required to make sure that no confidential data or information of other clients, or confidential Company data is displayed.
- Users are required to always use the highest security settings during all video conferences.

3.3.14. MOBILE DEVICES

The Company provide end-user computing devices including workstations, laptops, tablets, and smart phones which connect to the Company's network. These devices must be configured to:

- The Company's licensed anti-virus software with automatic definition update to ensure that the device is protected from malicious code.
- Automated patching process to ensure that operating systems and applications are kept up to date.
- Device timeouts and password/PINs/biometric setting to minimise the risk of unauthorised access to the device.
- Full disk encryption.

Users must diligently protect mobile computing or storage devices from loss or disclosure of Personal Information belonging to or maintained by the Company.

Confidential Information and data must not be downloaded to mobile or off-site computing devices, or storage devices.

Mobile computing or storage devices that contain Confidential Information must use encryption or equally strong measures to protect the data while it is being stored. Individual folders can be encrypted using instructions provided in encryption software.

3.3.15. PASSWORD PROTOCOLS

- A selected Password Management System must be used by each User in the Company.
- Users must use unique passwords on all systems, website logins and applications.
- Passwords shall not be displayed or transmitted in clear text and shall be suitably protected.
- Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the reuse of passwords.
- Default accounts shall be disabled, and default passwords associated with such accounts shall be changed.
- All Users will be requested to password protect their computers.
- The password should be kept secret and not given to any other user.
- Users should ensure that they log out when moving away from their desk for any purpose.

3.3.16. IT SECURITY

A User must:

- Use only those computing and IT resources of the Company for which authorisation has been given.

- Use computing and IT resources of the Company only for their intended purpose.
- Always lock computers and mobile phone when not directly in use.
- Stay alert and always report any suspicious activity to the Company.
- Always password-protect sensitive files on computers, USB flash drives, smartphones, or laptops.
- Always create complex passwords by including different letter cases, numbers, and punctuation. A User must also use different passwords for different websites and computers.
- Always ensure that, when plugging in personal devices such as USB's, MP3 players and smartphones, the device in question is not infected with a virus.
- Be cautious of suspicious emails and links. A User must always delete suspicious emails and never click on links or attachments.
- Exercise caution when forwarding email or messages, as some information that is intended for a specific individual may not be appropriate for general distribution.

A User must not:

- Be tricked into giving away Confidential Information by responding to emails or calls requesting Confidential Information or Personal Information.
- Use an unprotected computer to access the Company's systems.
- Leave Confidential or Personal Information in view of any person that should not have access to such information.
- Install unauthorised programs on any Company computer.
- Furnish false data on any sign-up form, employment contract, or online application.
- At any time misrepresent their identity, use an anonymous identity or someone else's identity, password or identity number, or address.
- Attempt to circumvent the user authentication or security of any host, network, or account. This includes, accessing data not intended for the User, logging into a server or account that the User is not expressly authorised to access, or probing the security of other networks.
- Seek loopholes in computer security systems or attempt to gain knowledge of any password, or any other information used for authentication purposes. This may also not be done to attempt to damage computer systems, obtain extra resources, take resources from another User, gain access to systems or use systems for which proper authorisation was not given.
- Use any program, script, or command, or send messages of any kind, designed to interfere with another User's session.
- Execute any form of network monitoring which may intercept data not intended for a specific User's use.

3.3.17. USER DEACTIVATION

Deactivation of a User's access will take place in the following circumstances:

- When the User is an employee and has resigned from the Company.
- When the User has been authorised to assist on a Company project and the project in question has been finalised.
- Where the User is an employee has been suspended from the Company.

Deactivation of access will take place as soon as possible, but not longer than 24 hours from the time that a decision has been made by the Company to deactivate a User.

3.3.18. PRIVACY AND CONFIDENTIALITY

The following will be deemed to be a breach of privacy and confidentially:

- Transmission, distribution, processing or storage of any information, data, or material in violation of POPIA or any other applicable privacy laws or regulations.
- A violation or infringement of any intellectual property right of any nature whatsoever.

- A contravention of the privacy rights of any natural person or juristic person under POPIA or any other applicable privacy laws or regulations.

3.3.19. EMPLOYEE ACKNOWLEDGEMENT

As a requirement of IT system access, and as a component of security awareness training, all Users, whether employees of the Company or third parties, will be required to provide signed acceptance of this Policy, confirming such User's acknowledgement that they are bound by all provisions set out in this Policy. A copy of the signed document will be provided to the User in question, and the original will be retained by the Company.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.4. Policy: Backup and Restoration

3.4.1. PURPOSE

The Company set is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems. The backup and restoration of data is an important aspect to ensure the availability of information and data for the Company.

3.4.2. OBJECTIVE

The objective of this Policy is to formalise the backup and restoration process adopted by the Company. The process of backing up data is pivotal to a successful Disaster Recovery Plan (DRP).

3.4.3. SCOPE

This Policy applies to employees, contractors, visitors, and other persons (User) authorised to access and use the Company's systems. This Policy covers all servers, workstations, network devices, operating systems, applications, and other information assets belonging to the Company.

3.4.4. TERMS AND ABBREVIATIONS

- **Backup** means the copying of physical or virtual files or databases to a secondary location for preservation to assist in the event of equipment failure or catastrophe.
- **Restoration** means the process of restoring something to its former condition and, in the case of a computer or other electronic device, means returning it to a previous state, including restoring a previous system backup or the original factory setting, or restoring data that was on the system.

3.4.5. POLICY

The extent, frequency and retention period of backups must reflect:

- The Company's business requirements.
- The Company's security requirements of the information involved.
- How critical the information is to the Company's continued business operations.
- The retention period for essential business information.
- Any requirement for archived copies to be permanently retained by the Company.

The extent, frequency and retention periods of the Backups must be reviewed regularly. The Company's critical systems must be clearly identified, and the Backup arrangements must cover all system information, applications, and data necessary to recover the complete system in the event of a disaster. Where backup arrangements are automated, such automated solutions must be sufficiently tested prior to implementation and at regular intervals thereafter.

All backup media must be labelled with dates and codes which enables easy identification of the source of the data and the type of backup used on the media.

Where the confidentiality of the information is important, backups must be protected by encryption and all encryption keys must be always kept securely. Clear procedures must be in place to ensure that backup media can be decrypted as required.

Complete records of the backup copies must be retained both locally and remotely and afforded physical and environmental protection. Such records should include information pertaining to the data location, date of backup, type of backup and the like. Copies of backup media must be removed from

all Company devices as soon as reasonably possible when a backup or restoration has been completed.

Backup media, which is retained on-site at the Company, must be stored securely at a sufficient distance away from the original data source to ensure that both the original and backup copies are not compromised. Access to the backup media must be restricted to authorised staff only. All backups identified for long term storage must be stored at a secure remote location with appropriate protection to ensure continuing media integrity.

Restoration processes must be checked and tested regularly to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

Hard copy paper files containing important information and data must also be digitised (scanned) and stored in a location where they will be backed up by the Company in the same manner as electronic information.

Backup data and media no longer required, must be clearly marked and recorded for secure disposal or destruction, with due environmental consideration.

3.4.6. PROCEDURE

There are 5 common types of backups:

Full Backup	A Full Backup is when every single file and folder in the Company's systems is backed up. A Full Backup takes longer and requires more space than other types of backups. However, the process of restoring lost data from the backup is much faster
Incremental Backup	With Incremental Backups only the first backup is a Full Backup. Subsequent backups only store changes that were made after the previous backup. The process of restoring lost data from the backup is longer, however, the backup process itself is much quicker.
Differential Backup	A Differential Backup is like an Incremental Backup. With both, the first backup is full and subsequent backups only store changes made to files after the last backup. This type of backup requires more storage space than an Incremental Backup does, however, it also allows for a faster restoration time.
Mirror Backup	A Mirror Backup is when an exact copy is made of the source data. The advantage of Mirror Backups is that old, obsolete files are not being stored. When obsolete files are deleted, they are also deleted from the Mirror Backup when the system backs up. The disadvantage of a Mirror Backup is that, if files are accidentally deleted, they may also be lost from the backup.
Replication Backup	A Replication Backup occurs where data stored on servers is replicated between different servers. Sometimes these servers may be in the same data centre. If the backup is a pure replication, there is a risk that if the data on the main server is corrupted, the rest of the replicated data could also be corrupted. When implementing Replication Backups, a backup that is at least 1 day older than the live data must be kept managing this risk.

3.4.7. BACKUP SCHEDULE

The Backup schedule of the Company must be reviewed and updated on a regular basis. The Backup Schedule must contain the following information:

- The system and device to be backed up.
- The location of such device.
- The type of backup that was implemented.
- The frequency of the backup
- The person responsible for the backup.

3.4.8. USER'S RESPONSIBILITIES

- Users must ensure that data is securely maintained and is available for backup.
- Users must store any data and files that require backup on their allocated network storage area and not on local hard drives.
- If the allocated storage area becomes unavailable, Users may not temporarily save the data locally on hard drives or on a USB data stick.

3.4.9. DATA RESTORATION

Data Restoration must only be done by competent, authorised staff within the Company.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.5. Policy: Bring Your Own Device (BYOD)

3.5.1. PURPOSE

Bring your own Device (BYOD) is the practice of allowing employees and other authorised persons that perform work for the Company, to use their own personal devices for work purposes. This includes mobile phones, laptops, and tablets. The use of such personal devices for Company purposes will be referred to as BYOD.

It is important for the Company to protect and secure the data or information that it processes to ensure compliance with the provisions of POPIA. The purpose of this Policy is to set out how the Company will retain control over its information while such information is being accessed through devices that are not owned by the Company.

3.5.2. PERSONAL USE

The computers, electronic media and services provided by the Company are primarily for business use to assist Users in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable. All such use should be done in a manner that does not negatively affect the systems' use for their business purposes. Users are expected to demonstrate a sense of responsibility and not abuse this privilege.

3.5.3. SCOPE

This Policy applies to all employees, contractors, visitors, or other persons authorised to use the Company's systems (Users), that make use of personally owned devices to process, store or transfer any information for purposes of conducting business for the Company. This Policy applies to all Users irrespective of whether they make use of personal devices for Company business at the premises of the Company or remotely.

3.5.4. POLICY

The Company supports the use of BYOD for work purposes. The Company restricts the use of BYOD only to a limited number of Users who would not otherwise be able to perform their work. All information belonging to the Company that is stored, transferred, or processed on BYOD devices remains under the Company's ownership, and the Company retains the right to regulate such information, and the processing of it, even though it is not the owner of the BYOD.

3.5.5. ACCESS TO EMPLOYEE COMMUNICATIONS

Generally, electronic information created and communicated by Users using e-mail, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access, and similar electronic media is not reviewed by the Company. However, the following conditions should be noted: The Company does routinely gather logs for electronic activities or monitor User communications directly, e.g., telephone numbers dialled, sites accessed, call length, and time at which calls are made, for the following purposes:

- Cost analysis.
- Resource allocation.
- Optimum technical management of information resources.
- Detecting patterns of use that indicate Users are violating company policies or engaging in illegal activity.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.5.6. PROCEDURES

Permitted use of BYOD.

The Company will create a list of Users with job titles, if Users are employees, or relationship to Company, if Users are not employees, together with the applications and databases they can access with their own personal device.

Refer to Annexure A: List BYOD Devices

Only Users that need information to perform their duties effectively with a BYOD device will be granted permission to use their own devices in terms of this Policy.

Permitted devices.

The Company will create and maintain a list of acceptable devices which can be used as BYOD, together with mandatory settings to be deployed for each device.

Refer to Annexure A: List BYOD Devices

Hardware and Software

To prevent computer viruses from being transmitted through the Company's IT system, downloading of any unauthorised software is strictly prohibited on BYOD devices. Only software registered through the Company may be downloaded. Users should contact the Information Officer if they have any questions.

- The Company only permits the use of duly licensed software for its IT systems and BYOD devices.
- The Company also requires that all software that may be used must be “virus free”.
- No user may bring any hardware or software for use on the Company IT systems, without the specific permission of management or the Information Officer.

Acceptable usage

In addition to the provisions contained in the Acceptable Usage Policy, the following requirements are mandatory for every BYOD User:

- Users must set and use a strong passcode to access BYOD devices.
- Users must not share passcodes with anyone else.
- Users must set devices to lock automatically when the device is inactive for more than 5 minutes.
- The latest and most secure antivirus software must be installed on each device and updated regularly.
- Patches and updates to operating systems of devices must be installed regularly.
- Each device must be configured to enable the device in question to be remotely wiped should it be misplaced.
- Personal Information, sensitive, critical, confidential, and proprietary information of the Company must be protected by the most stringent security measures available (such as two pin authentication or encryption).
- When using BYOD off the Company premises, Users must ensure that all devices are not left unattended, and these should be physically locked away.
- When using BYOD in public places, Users must ensure that no Company information can be read by unauthorised persons and that BYOD devices are encrypted.
- Users must notify the Information Officer before any device used in the BYOD initiative is being disposed of, sold, or handed to a third party for servicing.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Prohibited uses of BYOD's.

BYOD Users are prohibited from doing the following:

- Allow anyone else access to the device in question.
- Install unknown and untrusted applications.
- Store illegal material on the device.
- Install unlicensed software.
- Connect via Bluetooth to any unknown devices.
- Connect to unknown Wi-Fi networks.
- Locally store passwords.
- Configure logins to save passwords for applications.
- Locally store any information that is Personal Information or Confidential Information.
- Transfer any Company information to any unauthorised devices, including private or home devices.

Special rights

The Company has the right to view, edit, and delete all Company information that is stored, transferred, or processed on a BYOD without the consent of the owner of the device in question.

Reimbursement

The Company will pay for the following:

- Software required by the Company to manage and control Company related information stored on any authorised device.
- Other approved applications required to fulfil the duties or responsibilities of the relevant User.

Security breaches

All security breaches related to BYOD must be reported immediately to the Information Officer. This includes the loss or theft of any unencrypted devices.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.6. Policy: Clean Desk and Clear Screen

3.6.1. PURPOSE

The purpose of this Policy is to ensure that all paper and electronic records containing Personal Information, or Confidential Information are secured when not in use, and are not left visible on an unattended desk and screen. If the User is working on any Company system or device remotely, such User must also ensure that the provisions of this Policy are always adhered to.

Controlling physical access to the information within the Company is important. This relies upon physical, technological and policy controls to ensure that the Company operates within a secure environment, protecting personnel, facilities, information, and data from the risk of:

- Loss or damage of information resources.
- Unauthorised access to information resources.
- Disruption or destruction of information processing facilities.
- Breach of relevant legislation, including POPIA, or non-compliance with regulatory standards.

3.6.2. SCOPE

This Policy applies to all Users, and any functions within the Company where Personal Information or Confidential Information are created, accessed, updated, stored, maintained, managed, or even deleted.

3.6.3. POLICY

All Users are required to apply a clean Desk and Clear Screen Policy, as this will help to protect the Company's information assets from being compromised. The following actions must be taken to ensure that the necessary controls are in place:

- Users must ensure that all Personal Information or Confidential Information stored in both hardcopy or electronic form, is secured in their desk at the end of each day, or when they are expected to be away from their desk.
- Screens must be locked when a User's desk is unoccupied.
- All Personal Information and Confidential Information must be locked in a drawer or cupboard at the end of each day or when the desk is unoccupied.
- Filing cabinets containing Personal Information and Confidential Information must be kept closed and locked at the end of each day, or when not in use or when unattended.
- Keys used to access Personal Information or Confidential Information must not be left at an unattended desk.
- Laptops must be either locked with a secure locking mechanism or locked away in a drawer or cabinet at the end of each workday or when they are left unattended.
- Passwords may not be left on any sticky or other notes posted on or under a computer or laptop, nor may they be left written down in an accessible location.
- Printouts containing any Personal Information or Confidential Information must be removed from the printer immediately.
- All Personal Information and Confidential Information that is ready to be disposed of must be shredded or otherwise securely destroyed.
- Whiteboards containing Personal Information or Confidential Information should be erased as soon as reasonably possible.
- All mass storage devices, including CDROMs, DVDs or USB drives must be treated as sensitive and must be secured in a locked drawer.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.7. Policy: Physical and Environmental Security

3.7.1. PURPOSE

The purpose of this Policy is to minimize the potential exposure to the Company's documents from damages which may result from unauthorised access to the resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical Company internal systems, etc.

This Policy sets out the requirements for protecting the information and technology resources and assets of the Company from physical and environmental threats to reduce the risk of loss, theft, damage, and unauthorised access to those resources.

3.7.2. POLICY

The Company's property, information and technology resources and assets should have sufficient physical and environmental security controls applied to mitigate the risks to these assets. Such risks include fire, natural disasters, burglary, theft, vandalism, and terrorism (physical security risks), and electrical surges, flooding, and natural disasters (environmental security risks).

3.7.3. PHYSICAL SECURITY

Appropriate physical security measures must be implemented in relation to the type of information or data that is required to be protected. For example, where there is an area within the Company's premises that visitors can access, but where no Personal Information of the Company is kept, a lower level of physical security will be required than for an area where Personal Information is stored or processed.

Appropriate physical controls must be implemented in all areas within the Company's premises. The areas in the premises should be classified as follows:

- Public areas such as the reception and the canteen may be classified as a low risk.
- Controlled areas such as general working areas or boardrooms may be classified as a medium risk.
- Highly restricted areas such as the Information Technology Department, server room, Finance Department, Human Resources Department, and other areas where Personal Information, and Confidential Information are processed, may be classified as high risk.

Physical security measures must be implemented which will include:

- Access control to the Company's premises.
- An armed response that can be activated in the case of an emergency. (*If applicable*)
- Alarm systems that will be activated when the building is unoccupied to ensure intrusion detection. (*If applicable*)
- Controlled access by employees and authorised third-parties.
- Network wiring and equipment rooms and cabinets must be locked when unattended.
- Devices should likewise be physically secured when unattended.
- All office doors must remain locked after hours or when offices are unattended.
- Mobile storage devices must be stored securely when unattended.

Encrypting data stored on mobile devices, such as whole disk encryption on computers, reduces the risk of a data breach resulting from theft, loss, or unauthorised access. When Users travel with mobile storage devices or use them in public places, security precautions must be taken to prevent loss, theft, damage, or unauthorised access to such devices. This includes the use of tracking and recovery software on laptop computers, tablets, and mobile phones.

For purposes of this Policy, secure storage methods include storage in a locked cabinet or closet, or storage in a locked office.

3.7.4. PHYSICAL ACCESS TO FILES

- Company files must be stored in a lockable safe, to which only authorised Users has access.
- No copying of the any documents containing Personal Information is allowed for any use outside the offices of the Company.
- All Personal Information must be regarded as highly confidential, especially if consolidated or summarised in any way.
- Only Users who have permission to access Personal and Confidential Information, may have access to it and no other persons may see that information, unless the necessary legal Company Confidentiality Agreements has been signed.
- The distribution of reports must be strictly controlled to ensure confidentiality.
- Any information sent to an outside organisation must be approved and verified, the recipients confirmed, and the way the data will be deployed must be cleared by the Information Officer.
- Any hard copy of consolidated or summarised information must be shredded when disposed of.
- All documentation is the sole property of the Company and may not be copied for private use.

3.7.5. ENVIRONMENTAL SECURITY

Some potential environmental risks include:

- **Water**: Areas where there is a risk of water damage due to flooding or bursting of geysers should be identified. Servers and other sensitive equipment that contain Personal Information, or Confidential Information should be kept away from these areas.
- **Electrical power**: Electrical power for servers hosting Personal Information, and Confidential Information must be protected by Uninterruptable Power Supplies (UPS) to ensure the continuity of services during power outages and protect equipment from damage due to power irregularities. Systems hosting such information must also be protected with a standby power generator, if reasonably possible.
- **Natural disasters**: All conceivable threats should be identified and mitigating controls should be put in place. An example of a control could be to install lightning equipment to prevent lightning from causing damage to the building that the Company occupies.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

3.8. Policy: Data Encryption

3.8.1 PURPOSE

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the South Africa.

3.8.2 POLICY

This policy applies to all Akili IT Services employees and subcontractors.

3.8.2.1 Algorithm Requirements

- Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.
- Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
- Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Consider RFC6090 to avoid patent infringement.
	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

3.8.2.2 Hash Function Requirements

In general, Akili IT Services adheres to the NIST Policy on Hash Functions.

3.8.2.3 Key Agreement and Authentication

- Key exchanges must use one of the following cryptographic protocols: DiffieHellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- End points must be authenticated prior to the exchange or derivation of session keys.
- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

3.8.2.4 Key Generation

- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.
- Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

POLICY COMPLIANCE

3.8.2.5 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

3.8.2.6 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

3.8.2.7 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.8.3 RELATED STANDARDS, POLICIES AND PROCESSES

National Institute of Standards and Technology (NIST) publication FIPS 140-2,

NIST Policy on Hash Functions

3.8.4 DEFINITIONS AND TERMS

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

SECTION 4: DATA SUBJECT ACCESS RIGHTS (DSAR) MANAGEMENT

4.1. Policy: Access to Personal Information

4.1.1. INTRODUCTION

The Company will provide accurate and timely information regarding its activities to its consumers, employees, suppliers, partners and stakeholders and other interested parties (Data Subjects). This Policy reflects the various capacities in which the Company operates, and the nature of the information it collects and processes in the daily activities of the Company. It also determines the level of disclosure applicable to different types of information and in particular Personal Information.

The Company's Access to Personal Information Policy requires the Company to implement and maintain reasonable safeguards to protect the personal privacy of Data Subjects and to protect the confidentiality of Personal Information.

4.1.2. OBJECTIVE

The objective of this Policy is to protect the Company information assets from threats, whether internal or external, deliberate, or accidental, to ensure business continuation, minimise business damage and maximise business opportunities.

This policy establishes a general standard on the protection of Personal Information within the Company, and it provides principles regarding the right of individuals to privacy and to reasonable safeguards of their Personal Information.

4.1.3. THE NINE RIGHTS OF A DATA SUBJECT

A Data Subject has the right to have their Personal Information processed in accordance with Chapter 3 of POPIA, including the right:

- To be notified that Personal Information about them is being collected as provided for in terms of Section 18, or their Personal Information has been accessed or acquired by an unauthorised person as provided for in Section 22.
- To establish whether the Company holds Personal Information of that Data Subject and to request access to their Personal Information as provided for in Section 23.
- To request, where necessary, the correction, destruction, or deletion of their Personal Information as provided for in Section 24.
- To object, on reasonable grounds to the processing of their Personal Information as provided for in Section 11(3)(a).
- To object to the processing of their Personal Information at any time for purposes of direct marketing in terms of Section 11(3)(b), and Section 69(3)(c).
- Not to have their Personal Information processed for purposes of direct marketing by means of electronic communications except as referred to in Section 69(1).
- Not to be subject to a decision which is based solely based on the automated processing of their Personal Information in term of Section 71.
- To submit a complaint to the Information Regulator regarding interference with the protection of the Personal Information as provided for in Section 74.

- To institute civil proceedings regarding interference with the protection of their Personal Information as provided for in Section 99.

4.1.4. PERSONAL INFORMATION OF CONSUMERS, SUPPLIERS, SERVICE PROVIDERS AND THIRD-PARTIES

The Company does not provide access to the following consumer, supplier, service provider and third-party information, except as permitted by the Data Access Policies:

- Personal Information of consumers, suppliers, services providers and other third parties.
- Financial and Credit Information of consumers, suppliers, services providers and other third parties.

4.1.5. INFORMATION HANDLING

Information, in electronic and physical formats, should be handled in accordance with the sensitivity, risk and classification of the information:

- Ensure Confidentiality Agreements are in place before sharing data externally.
- When emailing sensitive files externally, the files should be password protected or encrypted.
- Verify email addresses prior to sending any files.
- Files should only be copied to removable storage when necessary and the storage should be encrypted.
- Use restricted access storage areas whenever possible.
- Data disposal should be done in accordance with the *Document Retention and Destruction Policy*.

4.1.6. ACCESS CONTROL POLICY

- Access to information must be provided based on a need-to-know basis.
- All the Company's devices and computers must be password protected.
- Multi-factor authentication for remote access to Company networks by employees, administrators, and third-parties must be implemented where available.
- A Password Management System must be used by everyone in the Company.
- Only secure Wi-Fi connections may be used.
- The Company will make use of a Virtual Private Network (VPN) for access control and internet stability.
- A strict *Bring Your Own Device Policy* are implemented in the Company.
- All internal and external hard drives must be encrypted as per the Company's *Data Security Policy*.
- All electronic information, including Company operational information and Data Subjects' Personal Information, must be backed up as per the *Backup Policy* and Schedule.
- All backups must be encrypted.
- Access to physical files and paperwork will be controlled and limited. Physical files will be kept in a safe for security purposes and damage protection.

The following rules must be maintained for managing User access rights:

- Each system must have clear procedures for approval and method of granting access to that system.
- User access rights are subject to periodic reviews.
- Inactive user accounts must be disabled.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.2. Policy: Information Transfer

4.2.1. INTRODUCTION

This Policy regulates the transfer of information within and from and to the Company. Where the information being transferred consists of Personal Information, the provisions of POPIA will apply to the processing of information by or on behalf of the Company.

4.2.2. PURPOSE

There are many occasions when information is transferred between different departments of the Company, and between the Company and third-party service providers, clients, customers, and the like. This transfer of information is affected by a wide variety of media and methods, in both electronic and paper format. In every transfer of information, there is a risk that the information in question may be lost, misappropriated, or accidentally disclosed. Where the information in question is Personal Information, or confidential, sensitive, critical, or proprietary information of the Company, the risk to the Company increases significantly.

The Company has a duty of care in handling information. It is essential that the transfer of information is performed in a way that adequately protects such information. It is always the responsibility of the sender of information to assess the risks involved in the transfer of information and to ensure that controls are in place to mitigate such risks. This Policy outlines the responsibilities attached to, and the minimum-security requirements, for the transfer of information, including Personal Information, and Confidential Information.

This Policy applies to all areas in the Company where Personal Information, and Confidential Information is created, accessed, processed, updated, stored, maintained, or managed.

This Policy applies to all employees, contractors, visitors, and other persons (Users) authorised to access and use the Company's systems who are involved in the transfer of information.

4.2.3. POLICY

Electronic communication channels

The Company's information may be exchanged through the electronic communication channels, such as email. New data channels must be approved by the Information Officer prior to being implemented. The Information Officer's approval will set out the type of communication allowed, and controls pertaining to the use of the data channel. Public information may be made available to the public. All information meant for internal use only, may only be transferred to parties that are authorised by the Company to receive such information, and that are bound contractually not to disclose such information.

Where the information is classified as either Personal Information, or Confidential Information, the Company should ensure that such information is transferred in a secure manner and that only certain secure channels are used:

- Email may be used to transfer Personal Information, and Confidential Information only when such information has been sufficiently password protected or properly encrypted:
- A file transfer method may be used to transfer Personal Information, or Confidential Information only when a secure file transfer protocol channel is used.
- Portable Media (such as CDs, DVDs, USB drives and memory cards) may be used to transfer Personal Information, and Confidential Information only when such information on the device in question is properly password protected or encrypted.

- Telephonic communication, fax transmission, mobile voice or SMS communication, and social media may not be used to transfer or disclose Personal Information, or Confidential Information.

Non-electronic communication channels

The Company's information may be exchanged through the non-electronic communication channels outlined below.

Where the information is classified as either Personal Information, and Confidential Information, the guidelines set out below should be used to ensure that such information is transferred in a secure manner:

- Registered or normal post may not be used to transfer Personal Information, and Confidential Information.
- Letters delivered by hand may be used to transfer Personal Information, or Confidential Information only when the sender of such information ensures that the party receiving the information is properly identified and authorised to receive such information.

4.2.4. RESPONSIBILITIES OF THE SENDER AND RECEIVER OF INFORMATION

The sender's responsibilities for transferring Personal Information, and Confidential Information are:

- Assessing the information to be sent and ensuring that it is in line with the guidelines set out in this Policy.
- Ensuring that the identity of the receiver is known that such receiver is authorised to receive the information.
- Ensuring that the transfer of information is formally confirmed and documented.
- Ensuring that the information is sent and tracked in an appropriate manner to ensure compliance with this Policy.

The person receiving Personal Information, and Confidential Information is responsible for ensuring that:

- The information received is information that they have a right to receive.
- They fully disclose their identity.

4.2.5. RELATIONSHIP WITH EXTERNAL PARTIES

Before exchanging any information with any person or party outside of the Company, an agreement must be concluded between the Company and third-party. Such agreement must comply with POPIA and must contain at least the following clauses:

- Method of identification of the third-party.
- Confirmations or warranties regarding authorisation to access information.
- Technical standards and appropriate Data Channels for the transfer of information.
- Labelling and handling of Personal Information, and Confidential Information.
- Warranties from the third-party regarding compliance with POPIA and all other relevant privacy laws.
- Obligations on the third-party to safeguard the security of the information in question.
- Indemnities in favour of the Company in the event of a breach by the third-party of POPIA or the agreement itself.
- Protections for the Company's intellectual property rights.
- Incident responses and what must be done in the event of security breaches.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.2.6. TRANSBORDER PERSONAL INFORMATION FLOW

Technological developments in the field of information, computers and communications are leading to significant structural changes in the economy of South Africa. Flows of computerised data and information are an important consequence of technological advances and are playing an increasing role in national economies. With the growing economic interdependence of countries, these flows acquire an international dimension, known as Transborder Personal Information Flows.

Transborder transfer of information is subject to RICA (Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002), FICA (Financial Intelligence Centre Act, 2001), ECTA (Electronic Communications and Transactions Act, 2002) and the POPI Act, 2013.

The Company may not transfer Personal Information about a data subject to a third-party who is in a foreign country unless adequate levels of protection are provided by:

- The Law of the country.
- Binding Corporate Rules of the third-party to which Personal Information is provided.
- A binding Agreement between the Company and the third-party in the foreign country.
- The Law, Corporate Rules or Binding Agreement must uphold the principles of reasonable processing, like the Conditions of Lawful Processing in Chapter 3 of POPIA.
- The data subject consents to the transfer (*Refer to Annexure A*).

In view of the above, Chapter 3 of POPIA acknowledges that:

- Computerised data and information now circulate freely on an international scale.
- Recognises the diversity of participants in Transborder Personal Information Flows, such as commercial and non-commercial organisations, individuals, and governments.
- Recognising the wide variety of computerised data and information, traded, or exchanged across national borders.
- Recognises the growing importance of Transborder Personal Information Flows and the benefits that can be derived from transborder data flows.
- Recognises the national policies which affect Transborder Personal Information Flows.
- Is aware of the social and economic benefits resulting from access to a variety of sources of information and of efficient and effective information services.
- Recognises that member countries have a common interest in facilitating Transborder Personal Information Flows, and in reconciling different Policy objectives in this field.

The POPI Act has the intention to:

- Promote access to data and information and related services and avoid the creation of barriers to the international exchange of data and information.
- Seek transparency in Regulations and Policies relating to information, computer and communications services affecting Transborder Personal Information Flows.
- Develop common approaches for dealing with issues related to Transborder Personal Information Flows and develop harmonised solutions.
- Consider possible implications for other countries when dealing with issues related to Transborder Personal Information Flows.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.3. Policy: Direct Marketing

4.3.1. PURPOSE

Direct Marketing means to approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of *(Section 1 of the Protection of Personal Information Act 4 of 2013)*:

- Promoting or offering to supply any goods or services to the Data Subject.
- Requesting the Data Subject to make a donation of any kind for any reason.

POPIA includes specific requirements around direct marketing. The direct marketing requirement is the most public requirement of POPIA. Consumers have the right to specifically opt-in into direct marketing or request an opt-out of any direct marketing (*Refer to Annexure A*).

Direct Marketing is a well-established and accepted marketing medium. As such, the communication with the potential consumers should be factual, honest, decent, and informative, and should not violate any of the laws of the country. This Policy focus on two objectives:

- For those in direct marketing it lays down criteria for professional conduct.
- For the public it gives a clear indication of the limitations accepted by those using or working in direct marketing.

4.3.2. SCOPE

In the Company, Direct Marketing involves the following three aspects:

- Direct Marketing consists of any promotional, publicity or communications activity sent directly to individuals or companies intended to promote the Company's products and services.
- The Company carries out Direct Marketing in accordance with the Privacy Notice and legal requirements (*Refer to Annexure A*).
- This Policy should be read in conjunction with *Acceptable Usage Policy*.

4.3.3. USE OF DIRECT MARKETING

- The Company uses e-mail and e-marketing to send information directly to its business clients and contacts including insights, event invitations and news on products and services.
- This information is not sent automatically, and the consumer is not obliged to receive it.
- The Company operates an "Opt-in" option for its Direct Marketing (*Refer to Annexure C*). This means the consumer will only be sent and receive communications if they are current consumers or where the Company has the consumer’s consent to do so.
- The Company use text messaging, telesales, social media platforms or online communication platforms to carry out Direct Marketing.
- The Company may occasionally share Personal Information with trusted Third-Parties to help the Company deliver efficient and quality services. Any such recipients will be contractually bound to safeguard the data entrusted to them and will not contact the consumer to offer services.

4.3.4. DIRECT MARKETING TO BE RECEIVED FROM THE COMPANY

The Company will use and process data to send communications about:

- Events, including invitations to seminars, webinars, and networking events.
- Insights, relating to the topics which the consumer have indicated are of interest as part of the opt-in process.
- New products or services.

- News and Information about the Company.

4.3.5. CIRCUMSTANCES WHERE DIRECT MARKETING WILL BE RECEIVED

- The consumer will only receive communications from the Company if the consumer is a current client of the Company or have opted-in to receive these communications.
- The consumer will be invited by e-mail to opt-in online because:
    - The consumer is a client of the Company.
    - The consumer attended at an event, seminar or webinar hosted by the Company.
    - The consumer attended at a public event organised by the Company.
    - The consumer provided a business card directly to an employee of the Company.
    - The Consumer registered their contact details to obtain information from the Company's website.
    - The Company received an e-mail request from the consumer to attend an event the Company have advertised via social media or on the Website.
    - An employee added the consumer's details to the database due to an existing relationship.

The Company does not buy lists from third-parties to use for Direct Marketing.

4.3.6. REFUSAL OF RECEIVING DIRECT MARKETING INFORMATION

If the consumer would like to withdraw their consent or opt-out of receiving any Direct Marketing, they can do so using the Company's Unsubscribe Notice or Opt-Out options (*Refer to Annexure D*).

4.3.7. ACCURACY OF PERSONAL INFORMATION IN DIRECT MARKETING

The Company does not rely on consumer consent to receive Direct Marketing indefinitely. The consumer will receive an email from the Company at intervals of no less than 2 years. The consumer will be asked to re-confirm their consent and preferences, to ensure that the data the Company holds, such as contact details, are current and accurate (*Refer to Annexure B*).

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.4. Policy: Personal Information of Employees

4.4.1. PUPROSE

POPIA includes all Personal and Special Personal Information that the Company might have about job applicants, employees, and former employees (Employee).

This Policy must be read in conjunction with the *Acceptable Usage Policy*. Confidentiality Agreements and Non-Disclosure Agreements referred to in the Acceptable Usage Policy, will be found in the Annexure of this Policy as it relates to Employee Personal Information (*Refer to Annexure C and D*)

4.4.2. REGULATION

POPIA imposes several new responsibilities the Company in the processing of the Personal Information of Employees:

- The Company must appoint an Information Officer who needs to be registered with the Information Regulator.
- Personal Information may, subject to certain exceptions, only be collected by the Company directly from the Employee.
- The Employee must be informed why the information is collected (purpose) and who the intended recipients of the information are (*Refer to Annexure A*).
- Personal Information may only be processed for an explicit, specific, and lawful purpose (such as the conclusion of an Employment Contract).
- Personal information may not be kept for longer than necessary to achieve the purpose for which it was collected. This means, for instance, that personal information collected from an unsuccessful job applicant should be destroyed after the recruitment process has been finalised and a successful candidate appointed.
- Personal Information must be distributed in a way that is compatible with the purpose for which it was collected.
- Personal Information may not be distributed to other third-parties, for example, for marketing purposes.
- The Company must take reasonable steps to ensure that the information collected is accurate, up to date and complete (*Refer to Annexure B*).
- The Company must ensure that the personal information is protected against risks of loss, damage, destruction, or unauthorised access.
- The Employee must also be allowed to access their personal information and can demand that the information be corrected if it is found to be inaccurate.

4.4.3. CONFIDENTIALITY OF PERSONAL INFORMATION OF EMPLOYEES

Personal Information of the Employees as per the Company's HR Policies and Procedures are not disclosed and are kept confidential except per the explicit consent of the employee. This includes active and inactive employees. This includes:

- Personal Information, including personal employment records, medical information, and personal communications (including email).
- Information relating to employee appointment and selection process.
- Information relating to proceedings of the Company's internal conflict resolution mechanisms.
- Information relating to investigations of allegations of employee misconduct and personal conflicts of interest.

4.4.4. PROCESSING THE PERSONAL INFORMATION OF EMPLOYEES

POPIA provides for limited use of the Personal Information of the Employee:

- If the employee consents (*Refer to Annexure D*).
- When processing is necessary for purposes of employment, such as details of banking accounts to be able to pay the employee's salary, or for vetting relevant educational qualifications.
- If the Company has a legal obligation to perform processing, e.g., for tax purposes.
- To protect a legitimate interest of the Employee, for example, collecting personal information required by a retirement fund to which the Employee belongs.
- If it is necessary to pursue the legitimate interests of the Company or a third-party, for example, doing a check on the criminal record of someone who requires security clearance, or providing information to an external party whom the Employee has authorised to carry out deductions from her or his wage or salary.

4.4.5. SPECIAL PERSONAL INFORMATION

Additional protections apply to Special Personal Information of the Employee. This may only be processed if:

- The processing is carried out with the written consent of the Employee.
- The processing is necessary for the establishment, exercise, or defence of a right or obligation in law.
- The processing is necessary to comply with an obligation of international public law.
- The processing is necessary for historical, statistical or research purposes if this serves a public interest, e.g., disease control.
- The information has deliberately been made public by the Employee, e.g., on social media.

4.4.6 MEDICAL TESTING

Medical testing of the Employees can yield particularly sensitive information about the Employee. POPIA mirrors Section 23 of the Employment Equity Act which permits medical testing only if it is required or permitted by legislation. Also, if it can be justified in the light of medical facts, employment conditions, social policy, or the fair distribution of employee benefits or the inherent requirements of the job.

Testing for the Employee's HIV status is prohibited unless authorised by the Labour Court.

Psychological testing and other similar assessments (such as psychometric tests) are also prohibited unless certain requirements are met, i.e., the test has been scientifically proven to be valid and reliable and that it can be applied fairly to all employees and is not biased against any employee or group of employees.

4.4.7 RIGHTS OF EMPLOYEES IN RESPECT OF THEIR PERSONAL INFORMATION

The Employee has the right to:

- Be notified by the Company that their Personal Information will be collected or has been accessed or acquired by an unauthorised person, i.e., someone who does not have consent to process the information.
- Establish what information the Company holds.
- Request access to such information.
- Request the correction, destruction, or deletion of personal information.
- Object on reasonable grounds to the processing of their Personal Information.

- Submit a complaint to the Regulator or institute civil proceedings to protect their rights under POPIA.

4.4.8 IMPLEMENTATION

The Company will implement the following standards regarding the processing of Personal Information of Employees:

- Issue an Employee Notification regarding the POPI Act.
- Conduct Employee Awareness Training on the POPI Act and Acceptable Usage under the POPI Act.
- Implement a Privacy Statement that:
    - Mentions the circumstances under which Personal Information may be collected and what may it be used for.
    - States what kinds of Personal Information may be collected and to which internal and external recipients the Personal Information may be supplied to.
    - States if the information may be distributed or stored outside of the country's borders.
    - Includes a general description of the of information security measures (such as fire walls) that will be implemented to ensure that the information is not accessible by unauthorised parties.
- Develop standard clauses on data protection in Employment Contracts and provide for Employee Consent to disclosure of information (*Refer to Annexure A-E*).
- Conduct an audit in respect of Personal Information currently being held, where such information is being held and for how long it has been held.
- Report data breaches to the Information Regulator and Employees concerned.
- Do not share any Personal Information unless it would be permissible to do so in terms of the Act.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.5. Policy: Data Operators

4.5.1. PURPOSE

The control of risks introduced into the Company by contractors, service providers, accountants, consultants, third-parties and suppliers (Data Operators) is an important element of the Company risk management system. For the purposes of this Policy Data Operator means any organisation whom the Company pays in return for any type of goods or service, or the processing of Personal Information. Selection criteria for Data Operators are dependent on the nature of the goods or services to be supplied and are determined by the Company policies and procedures plus statutory requirements.

This Policy defines the duties of the Data Operator in terms of the processing of Personal Information on behalf of the Company in compliance with the Protection of Personal Information Act, No.4 of 2013.

This Policy must be read in conjunction with the *Acceptable Usage Policy*. Confidentiality Agreements and Non-Disclosure Agreements referred to in the Acceptable Usage Policy, will be found in the Annexure of this Policy as it relates to Data Operator Personal Information as well as processing of Personal Information by Data Operators (*Refer to Annexure C and D*)

4.5.2. INTRODUCTION

If the Company uses Data Operators to process Personal Information, it must comply with Sections 20 and 21 of the Protection of Personal Information Act. POPIA requires the Company to enter into a written agreement with a Data Operator that processes Personal Information for the Company. The Company must ensure that such Data Operator maintains the security measures required by POPIA.

4.5.3. GUIDANCE FOR REVIEWING & MONITORING DATA OPERATORS

POPIA and Data Security Policies
The first stage in the process is to see if the Data Operator has the right attitudes to the security of Personal Information, and this is done by checking their policies.

Competence
Next a check should be carried out to ensure that the Data Operator are capable of processing Personal Information in a responsible manner and supplying services that meet appropriate legal requirements.

Standards
Once it is established that Data Operator can work in accordance with POPIA requirements, the Company needs to check that the product or service the Data Operator will supply is of a high enough standard.

Monitoring
Checks on policies, competence and standards must take place before the Data Operator's 'offer' (usually a quote, whether verbal or written) is accepted by the Company. There will be a need to monitor Data Operators' work to ensure that they are complying with the agreed methods and risk control measures. Also, that execution of the service is performed in accordance with proposed methods and control measures. Verification of the service takes place throughout service delivery. These checks complete the selection process. As soon as verification that the purchased product or

services meet specified POPIA requirements is completed, the Data Operator can then be contracted under the Company's existing day-to-day POPIA controls.

4.5.4. DATA OPERATOR DUTIES

The Data Operator agrees to the following (further details of which can be found in the section headed *Information Processing Agreement* (*Refer to Annexure E*)):

- Only use and disclose the Personal Information in accordance with the Company's specific written instructions.
- Take reasonable and appropriate, organisational, and technical security measures to protect Personal Information supplied by the Company or otherwise made available to the Data Operator.
- Permit the Company to audit the Data Operator in terms of its compliance with Sections 19 to 21 of POPIA.
- Comply with requests by the Company for access to Personal Information following the receipt of a valid and approved Data Subject Request.

The Data Operator is not permitted to sub-contract any of the processing of the Personal Information supplied by the Company, without first:

- Ensuring the sub-contractor will be compliant with the requirements of Sections 19 to 21 of POPIA.
- Obtaining prior written permission of the Company.

The Data Operator must also agree to co-operate with any action required to fulfil the requests or demands of the Information Regulator as outlined in POPIA, whether directly by the Information Regulator or indirectly by the Company.

4.5.5. RIGHTS OF THE COMPANY

An audit of the compliance of the Data Operator with Sections 19 to 21 of POPIA to be conducted by the Company, may include but is not limited to:

- Ensuring that the Data Operator transfers data securely.
- Ensuring that the Data Operator reports any security breaches or other problems to the Company.
- In any other way fulfil the duties of the Company as outlined in Section 21 of POPIA.

4.5.6. TERMINATION OF INFORMATION PROCESSING AGREEMENT

In terms of processing of Personal Information:

- Where the Data Operator is found by the Information Regulator to have not fulfilled its obligations in terms of compliance with POPIA, the Company has the right to cancel the Information Processing Agreement with the Data Operator with immediate effect.
- Whether for fault or any other termination reason, the Data Operator must return all Personal Information processed on behalf of the Company without delay, unless the Data Operator is required to retain such records in terms of other legislation or regulations.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

1. DEFINITIONS

Term used	Definition source
Data Operator	An operator means a person who processes Personal Information for or on behalf of a Company in terms of a contract or mandate, without coming under the direct authority of that party (*Section 1 of the Protection of Personal Information Act 4 of 2013).*
Personal information	Personal information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including: • Information relating to the 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. • Information relating to 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 assignment to the person. • The biometric information of the person. • The personal opinions, views, or preferences of the person. • Correspondence sent by the person. • 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. *(Section 1 of the Protection of Personal Information Act 4 of 2013)*
Processing	Processing means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including • The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use. • Dissemination by means of transmission, distribution or making available in any other form. • Merging, linking, as well as restriction, degradation, erasure, or destruction of information. (*Section 1 of the Protection of Personal Information Act 4 of 2013)*
Regulator or Information Regulator	There is hereby established a juristic person to be known as the Information Regulator, which: • Has jurisdiction throughout the Republic. • Is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour, or prejudice. • Must exercise its powers and perform its functions in accordance with this Act and the Promotion of Access to Information Act. • Is accountable to the National Assembly. (*Section 39 of the Protection of Personal Information Act 4 of 2013)*
Responsible Party	As defined in Section 1 of the Act: A Responsible Party is a body or person who determines the purpose of and means for processing Personal Information. Included in this definition are juristic persons (e.g., companies and businesses), whether they are public or private organisations (*Section 1 of the Protection of Personal Information Act 4 of 2013).* *In this Agreement it refers to Akili IT Services (Pty) Ltd (the Company)*

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Security safeguards	The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent: • loss of, damage to or unauthorised destruction of personal information. • unlawful access to or processing of personal information. The responsible party must take reasonable measures to: • identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control. • establish and maintain appropriate safeguards against the risks identified. • regularly verify that the safeguards are effectively implemented. • ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations. (*Section 19 of the Protection of Personal Information Act 4 of 2013)*
Sub-operator	Authorised sub-contractor working on behalf of the Operator
POPI / POPIA/ The Act	Protection of Personal Information Act, No.4 of 2013.

2. RELEVANT SECTIONS OF PROTECTION OF PERSONAL INFORMATION ACT, ACT, No. 4 OF 2013

CHAPTER 3 CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Security measures on integrity and confidentiality of Personal Information

(1) A Responsible Party must secure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:
- *(a) loss of, damage to or unauthorised destruction of Personal Information; and*
- *(b) unlawful access to or processing of Personal Information.*

(2) In order to give effect to subsection (1), the Responsible Party must take reasonable measures to—
- *(a) identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;*
- *(b) establish and maintain appropriate safeguards against the risks identified;*
- *(c) regularly verify that the safeguards are effectively implemented; and*
- *(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.*

(3) The Responsible Party must have due regard to generally accepted Information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Information processed by operator or person acting under authority.

20. An operator or anyone processing Personal Information on behalf of a Responsible Party or an operator, must:
- *(a) process such Information only with the knowledge or authorisation of the Responsible Party; and*
- *(b) treat Personal Information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.*

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Security measures regarding Information processed by operator.

21. (1) A Responsible Party must, in terms of a written contract between the Responsible Party and the operator, ensure that the operator which processes Personal Information for the Responsible Party establishes and maintains the security measures referred to in section 19.

(2) The operator must notify the Responsible Party immediately where there are reasonable grounds to believe

that the Personal Information of a data subject has been accessed or acquired by any unauthorised person.

3. INTRODUCTION

This Company and Operator Agreement is supplementary to the existing agreement between the Company and the Data Operator signed on the _____for the purpose of offering services to the Company. (*List services*):

_____

_____

_____

_____

a) In the case of the Company:

Company Name:	
Company Registration Number:	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

b) In the case of Data Operator:

Data Operator Name:	
Data Operator Registration Number:	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

This document defines the duties of the Operator in terms of the processing of Personal Information under the rights of the Company in compliance with the Protection of Personal Information Act, No.4 of 2013.

- Whereas the Company is required to adhere to the provisions of POPIA.
- Whereas the Data Operator collects, transmits, stores, or processes the Company Personal Information.
- Whereas the Data Operator could impact the security and confidentiality of the Company Personal Information in the performance of the services it provides to the Company.

4. DATA OPERATOR DUTIES

The Data Operator agrees to:

1. Comply with the security measures as referred to in Section 19 of the POPI Act.
2. Comply with the processing conditions as referred to in Section 20 of the POPI Act.
3. Comply with the security measures as referred to in Section 21 of the POPI Act.
4. Allow the Responsible Party to fulfil its duties as stated in Sections 19 to 21 of the POPI Act.

5. DATA OPERATOR COMPLIANCE WITH PRIVACY AND INFORMATION SECURITY REQUIREMENTS.

- The Data Operator must comply with all privacy laws as they relate to Personal Information.
- The Data Operator confirms that no applicable law, or Information Security enforcement action, investigation, litigation, or claim prohibits the Data Operator from fulfilling its obligations under the Agreement with the Company.
- The Data Operator shall enter any further privacy, Information security, Personal Information Transfer or Personal Information Processing Agreement requested by the Company for purposes of compliance with applicable privacy laws.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

6. DATA OPERATOR PERSONAL INFORMATION SAFEGUARDS

- The Data Operator must maintain and implement a comprehensive written Information Security Programme that complies with applicable privacy laws, including POPIA.
- The Data Operator's Information Security Programme must include administrative, technical, physical, organisational, and operational safeguards and security measures to:
    - Ensure the security and confidentiality of Personal Information.
    - Protect against any anticipated threats or hazards to the security and integrity of Personal Information.
    - Protect against any Information Security Incident.
    - Encourage timely internal reporting of Information Security Incidents.
    - Facilitate appropriate response by the Data Operator to Information Security Incidents.
- The Data Operator's Information Security Policies shall provide for:
    - Regular assessment of the risks to the security of Personal Information and systems used by the Data Operator to Process Personal Information.
    - Identification of internal and external threats that could result in an Information Security Incident.
    - Assessment of the potential damage of such threats, considering the sensitivity of such Personal Information.
    - Assessment of Policies, Procedures, and Information Systems of the Data Operator, to control risks.
    - Protection against such risks.
- If the processing by the Data Operator, involves the transmission of the Personal Information over a network, the Data Operator must protect the Personal Information against the risks of such a transmission.
- The Data Operator must exercise supervision over its employees to maintain the privacy, confidentiality, and security of Personal Information.
- The Data Operator must provide training, regarding the privacy, confidentiality, and Information security requirements, to its employees who have access to Personal Information.
- Upon the expiration or termination of the Agreement, the Data Operator shall return to the Company every original and copy in every media of all Personal Information in the Data Operator's possession.
- If the law does not permit the Data Operator to deliver the Personal Information, the Data Operator warrants that it shall ensure the protection and confidentiality of the Personal Information and that it shall not use or disclose any Personal Information.

7. DATA OPERATOR INFORMATION REQUEST AND INCIDENT REPORTING

- The Data Operator must immediately inform the Company in writing of any requests for Personal Information received from the Company's employees, customers, or any Third-Party.
- The Data Operator must notify the Company immediately in writing of any subpoena or order by a government authority, seeking access to or disclosure of Personal Information.
- If the Data Operator becomes aware of any Information Security Incident, the Data Operator must, within 24 hours after becoming aware of the Incident, notify the Company's Information Officer, in writing.
- The Data Operator must specify the extent to which Personal Information was reasonably believed to have been compromised or disclosed.
- The Data Operator must investigate the Information Security Incident, preserve all documents, Personal Information and other Information related to the Information Security Incident.
- The Data Operator must provide the Company with an Incident Report.
- The Data Operator must cooperate with the Company.

- At the Company's request the Data Operator must cooperate with law enforcement, regulatory officials, credit reporting companies, and credit card associations investigating an Information Security Incident.
- The Company will make the final decision on notifying the Company's customers, employees, service providers and the public of an Information Security Incident.
- The Data Operator will be responsible for the costs associated with the performance of its obligations if the Information Security Incident did not result from the acts or omissions of the Company.
- The Data Operator must reimburse the Company for all Notification Related Costs incurred by the Company in connection with any such Information Security Incident.
- The Company will be responsible for the Data Operators' reasonable costs and expenses associated with the performance of its obligations if the Information Security Incident resulted from the acts or omissions of the Company.

8. RIGHTS OF THE RESPONSIBLE PARTY

An audit of the compliance of the Operator with Sections 19 to 21 of the POPI Act to be conducted by the Company or its authorised agent may include but is not limited to:

- Ensuring that the Operator makes appropriate security checks on its staff.
- Ensuring that the Operator transfers data securely.
- Ensuring that the Operator reports any security breaches or other problems to the Company.
- In any other way fulfil the duties of the Company as outlined in Section 21 of the POPI Act.

9. RIGHT TO MONITOR

The Company shall have the right to monitor the Data Operator's compliance with its Policies.

The Data Operator shall deal promptly with any enquiries from the Company relating to the Processing of Personal Information subject to the Company's Policies.

10. TERMINATION

Termination of the Agreement in terms of processing of Personal Information:

- Where the Operator is found by the Regulator to have not fulfilled its obligations in terms of compliance with the Act, the Company has the right to cancel the agreement with the Operator with immediate effect.
- Whether for fault or any other termination reason, the Operator must return or effectively destroy all personal information processed on behalf of the Company without delay, unless the Data Operator are required to retain such records in terms of other legislation or regulations.
- Termination of this Agreement will not affect the provisions, which are intended to continue to apply after termination.
- If there is any unresolved dispute between the parties arising out of or in connection with this Agreement, the parties agree first to attempt to resolve the dispute informally by negotiation, and as far as possible avoid any formal dispute resolution process.
- If the dispute is not so resolved, it shall be submitted to and decided by arbitration in terms of the Arbitration Act, 42 of 1965.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

11. MISUSE OF MICROSOFT PERSONAL DATA

The Data operator/Subcontractor is responsible for providing clear instructions and effective means for reporting any misuse of Microsoft Personal Data. This responsibility includes establishing accessible reporting channels and procedures that enable timely notification of any suspected or actual misuse. The Subcontractor must ensure that reports are promptly acknowledged, investigated, and addressed, and must keep Akili IT Services informed of the actions taken and any outcomes.

12. VARIATION OF CONTRACT TERMS

It is the duty of the Company to monitor any changes to the POPI Act and associated regulations and to ensure ongoing compliance with the Act. This may require amendment from time to time of this Agreement.

Signed on behalf of the Company:

Signed at _____ on this _____day of _____ 20_____

Company Representative Signature	Company Representative Full Name
Witness Signature	Witness Full Name

Signed on behalf of the Data Operator:

Signed at _____ on this _____day of _____ 20_____

Data Operator Representative Signature	Data Operator Representative Full Name
Witness Signature	Witness Full Name

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.6. Policy: Processing of Requests from Data Subjects

4.6.1. PURPOSE

All the sections of the Protection of Personal Information Act 4 of 2013 (POPIA) became effective on 1 July 2020. In POPIA, all Data Subjects have the right to request the Company to confirm whether the Company holds information about them.

This Policy is to regulate any requests by Data Subjects for any personal information, that the Company may process in relation to such Data Subject Request.

It must be understood that no information will be provided by the Company unless:

- The Data Subject has requested this in writing.
- The Data Subject has been properly identified.
- All other provisions set out in this Policy have been complied with.

4.6.2. OBJECTIVE

The objective of this Policy is to effectively assist Data Subjects that approach the Company so that the Company can provide them with a record or a description of their Personal Information that the Company may store on its systems.

4.6.3. DATA SUBJECT CONSENT

This notification should be done (*Refer to Annexure A and B*):

- When a new relationship, contract or agreement is entered into with the Data Subject.
- Annually to ensure that the Data Subject is aware of the Personal Information kept by the Company (*Refer to Annexure C*).
- Whenever there is a change in the Company's business, functions, or activities that impacts on the use of the Data Subject's Personal Information.

The Data Subject Notification confirms the purpose of the use of Personal Information and the specific Personal Information that is used by the Company and the reason for its use.

4.6.4. DATA SUBJECT WITHDRAWAL OF CONSENT

This notification relates to the withdrawal of processing of all Personal Information of the Data Subject, subject to the following:

- Data Subject completing the Company's Data Subject Consent Withdrawal Form (*Refer to Annexure D*).
- Reasons for withdrawal or objections to the processing of Personal Information in terms of POPIA Section 11(1)(d) to (f) are as follows:
    - Processing does not protect the legitimate interest of the Data Subject.
    - Processing is not necessary for pursuing the legitimate interests of the Company to whom the Information is supplied.

4.6.5. FORMAL REQUEST FROM THE DATA SUBJECT

A formal request from a Data Subject for information that the Company holds about them, must be made in writing accompanied with adequate proof of identification (*Refer to Annexure F and G*):

- A certified copy of the Data Subject's identity document or passport.
- Proof of residence.

Any employees, contractors, visitors, or other Data Operators, who receive a written request for data held by the Company, must forward it to the Information Officer of the Company immediately. A Data Subject has a right to request this information.

Akili IT Services will ensure the accuracy, completeness, and relevance of all Microsoft Personal Data for the stated purposes for which it was processed. Personal data must be monitored regularly to confirm its continued accuracy and relevance.

Akili IT Services will document all monitoring, review, and correction activities and provide evidence of such actions to Microsoft upon request.

4.6.6. PROCESSING THE REQUEST FROM THE DATA SUBJECT

Natural Person Data Subject requesting information.

The natural person Data Subject must request in writing (*Refer to Annexure F and G*):

- Whether the Company processes any of their Personal Information, and to view a record of such Personal Information.
- This written request must be sent to the Information Officer.
- The Information Officer will request a certified copy of the individual's ID or passport, and proof of residence.
- Once this has been received and verified, the Information Officer will then be authorised to release the Personal Information in question, unless the Company cannot release such information for good reason. Such a reason would be if granting the Data Subject access would interfere with the privacy of others or would result in a breach of confidentiality by the Company. The Company will always provide the Data Subject with written reasons if this is the case.

The Information Officer must:

- Record the Data Subject Request on the Company's request system (*Refer to Annexure H and I*).
- Safely store the certified copy of the ID and passport, and proof of address, either in a file in a locked cupboard or online in an encrypted folder which cannot be accessed by an unauthorised party.

Juristic Person requesting Information.

The Juristic person in question must request in writing (*Refer to Annexure F and G)*:

- Whether the Company processes any of its Personal Information, and to view a record of the Personal Information.
- This written request must be sent to the Information Officer.
- The Information Officer must then request an appropriate document to identify the Juristic person. For a company this will be certified copies of the following:
  - CIPC documents.
  - FICA documents for the company (including proof of business premises).
  - Directors' details and copies of all director's ID's or passports.
- Once such documents have been received, the Information Officer will then be authorised to release the personal information to the individual. Unless the Company cannot release such information for good reason, such as if granting the Data Subject access would interfere with

the privacy of others or would result in a breach of confidentiality by the Company. The Company will always provide the Data Subject with written reasons if this is the case.

The Information Officer must:

- Record the Data Subject Request on the Company's request system (*Refer to Annexure H and I)*.
- Safely store the certified copies of all the documents either in a file in a locked cupboard or online in an encrypted folder which cannot be accessed by an unauthorised party.

Update the Information of the Data Subject

The Data Subject may request the Company to correct or delete the Personal Information if it is (*Refer to Annexure F and G*):

- Inaccurate, irrelevant, excessive, out of date, incomplete or misleading.
- Has been obtained unlawfully.

The Data Subject may request the Company to destroy such record of Personal Information. If such a request is made, the Company must send this request to the Information Officer, who will then decide what action to take in respect of the Personal Information. If the information is destroyed or deleted, the Data Subject must be provided with credible evidence that this has been done.

If instructed to do so by the Information Officer, the User in question must advise the Data Subject of any adverse consequences of deleting of destroying any Personal Information, including whether this will have an impact on the Company's ability to provide goods and services to the Data Subject.

Timeline

As soon as a request for information has been received in writing and the Data Subject has been properly identified and verified, the Company will have 30 working days to provide the Data Subject with the information in question.

Cost of providing information.

Data Subjects have the right to contact the Company to (*Refer to Annexure J*):

- Confirm that the Company holds the Data Subject's Personal Information at no charge.
- Provide the Data Subject with access to any records containing the Data Subject's Personal Information or a description of the Personal Information that the Company holds, subject to payment of a prescribed fee under POPIA.
- Confirm the identity of third parties who have had, or currently have, access to the Data Subject's Personal Information, also subject to payment of a prescribed fee under POPIA.

Delivery method of the information

Information may be shared with the Data Subject under this Policy in the following ways:

- The information may be provided to the Data Subject in person, provided that the Data Subject must sign for the information received.
- The information may be emailed to the Data Subject to the address that that Data Subject has specified in writing. Any information provided by email must be password protected, provided that the password:
  - Must not be sent in the same email as the information.
  - Must be sent via a different application, preferably WhatsApp.

.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6.) A: PROTECTION OF PERSONAL INFORMATION ACT 2013: COVERING LETTER TO GO WITH DATA SUBJECT CONSENT FORM

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

POPIA AND DATA SUBJECT CONSENT TO PROCESS PERSONAL INFORMATION

Dear Consumer,

As a valued supplier, service provider or client to our Company, we currently hold your or your business' Personal Information for services rendered, goods supplied or previous registration on the Company Website.

To comply with the POPI Act, kindly sign the attached Data Subject Form and return to the address at the bottom of the form.

All Personal Information will be held securely and whenever the Company sub-contracts or outsources other organisations to process any of your Personal Information on our behalf, we will bind these service providers by way of a Data Operator Agreement to perform such processing of your Personal Information.

If you require any further Information or clarification, kindly contact the Information Officer.

Thank you for your co-operation.

With kind regards.

_____

The Information Officer of the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) B: DATA SUBJECT CONSENT FORM

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

DATA SUBJECT INFORMATION

Full Name:	
Date of Birth:	
ID nr / Passport Nr:	
Contact Nr:	
Email:	
Relationship to the Company:	

I confirm my consent to process my Personal Data and Information by the Company, named hereabove, for the purpose of (*Mark with X*):

	Supply of Goods
	Rendering of Services
	Purchase of Goods
	Contracting for Services obtained
	Other: Specify

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Consent is hereby granted from myself, the Data Subject, to the Company.

Signed at _____ on this _____day of _____ 20_____

Full Name:	
Signature:	

Kindly send this Data Subject Consent Form to the Information Officer of the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) C: VERIFICATION AND UPDATING OF DATA SUBJECT PERSONAL INFORMATION

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

Enclosed is your Personal Information that we have on record.

Kindly confirm that it is correct. If it is incorrect or requires updating, please amend it accordingly.

When completed, email to our Information Officer.

Changes in Personal Information

Full Name:	
Date of Birth:	
ID nr / Passport Nr:	
Contact Nr:	
Email:	
Relationship to the Company:	
Physical Address:	
Postal Address:	

If there are any further changes or updates, kindly use this form and e-mail to our Information Officer.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

If you require any further Information or clarification, kindly contact the Information Officer.

Thank you,

_____

Information Officer at the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) D: DATA SUBJECT CONSENT WITHDRAWAL FORM

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

I, (Data Subject Name) _____,
would like to withdraw my consent to process my Personal Information by the Company.

Therefore, the no longer has my consent to process my Personal Information for the purpose of

_____

_____
(specify legitimate reason of processing Personal Information), which was previously granted.

The withdrawal of consent does not affect the lawfulness of the processing activities up to this point.

Please provide the following Information to help us identify you in our systems:

My Personal Information, as Data Subject, is as follows:

Full Name:	
Date of Birth:	
ID nr / Passport Nr:	
Contact Nr:	
Email:	
Relationship to the Company:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

A copy of the following documentation as confirmation of my Personal Information is attached:

- Proof of Residential Address
- Certified copy of Identity Document

Signed at _____ on this _____day of _____ 20_____

Full Name:	
Signature:	

Kindly send this Withdrawal of Consent Form to the Information Officer of the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) E: DATA SUBJECT OBJECTION TO PROCESSING OF PERSONAL INFORMATION FORM

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

PoPI Regulatory Form 1 must be completed by the Data Subject where there is an Objection to the Processing of Personal Information in terms of Section 11(1)(d) to (f) where there is a processing breach of the following:

- Processing protects a legitimate interest of the Data Subject.
- Processing is necessary for the proper performance of a public law duty by a public body.
- Processing is necessary for pursuing the legitimate interests of the responsible party or of a third-party to whom the Information is supplied.

REPUBLIC OF SOUTH AFRICA

FORM 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]

Note:

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.*

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

A	DETAILS OF DATA SUBJECT
Name(s) and surname / registered name of date subject:	
Unique Identifier / Identity Number:	
Residential, postal, or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** ***(Please provide detailed reasons for the objection)***
Signed at ..... this ..... day of .....20..... …….…….. *Signature of data subject/designated person*	

Kindly send this Data Subject Objection to Processing Of Personal Information Form to the Information Officer of the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) F: ACCESS TO PERSONAL INFORMATION AUTHORITY FORM

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

To be completed by the Data Subject:

Please complete the form below and return to the Information Officer.

Personal Information:	
Record:	
Data Subject*:*	
Department:	
Filed:	
Personal Information under control of:	
Access Required by:	
Purpose of Access:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Data Subject Signature:	
Date:	

To be completed by the Information Officer:

Access Authorised by:	
Name of Information Officer:	
Information Officer Signature:	
Date:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) G: DATA SUBJECT REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION FORM

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

Kindly complete the form below and return to the Information Officer.

REPUBLIC OF SOUTH AFRICA

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION

IN TERMS OF
SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013
(ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request 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 box with an "x".

Request for:

☐ Correction or deletion of the Personal Information about the data subject which is in possession or under the control of the responsible party.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique Identifier / Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
C	**INFORMATION TO BE CORRECTED / DELETED**
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 UNDER THE CONTROL OF THE RESPONSIBLE PARTY.** *(Please provide detailed reasons for the request)*
Signed at ..... this ..... day of .....20……..... …… *Signature of data subject / designated person*	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) H: DATA SUBJECT WITHDRAWAL NOTIFICATION REGISTER

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

Signed at _____this _____ day of _____20____.

_____

Signature of **Information Officer** on behalf the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

DATE OF WITHDRAWAL	DATA SUBJECT NAME	SUBJECT REF / ACCOUNT NO.	PERSONAL INFORMATION RECORD / FORM	DATE CONSENT OBTAINED	WITHDRAWAL OF CONSENT YES / NO	REASON FOR WITHDRAWAL

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) I: DATA SUBEJECT PERSONAL INFORMATION REQUEST REGISTER

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

Signed at _____this _____ day of _____20____.

_____

Signature of **Information Officer** on behalf the Company

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

DATE OF WITHDRAWAL	DATA SUBJECT NAME	SUBJECT REF / ACCOUNT NO.	PERSONAL INFORMATION RECORD / FORM	DATE CONSENT OBTAINED	WITHDRAWAL OF CONSENT YES/ NO	REASON FOR WITHDRAWAL

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (4.6) J: FEES PROPOSED FOR DATA SUBJECT REQUESTS

Fees in respect of Private Bodies

1. The fee for a copy of the manual as contemplated in regulation 9(2)(c) is R1,10 for every photocopy of an A4-size page or part thereof.

2. The fees for reproduction referred to in regulation 11(1) are as follows:

(a)		For every photocopy of an A4-size page or part thereof	R 1,10
(b)		For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form	R 0,75
(c)		For a copy in a computer-readable form on -	
	(i)	stiffy disc	R 7,50
	(ii)	compact disc	R70,00
(d)	(i)	For a transcription of visual images, for an A4-size page or part thereof	R40,00
	(ii)	For a copy of visual images	R60,00
(e)	(i)	For a transcription of an audio record, for an A4-size page or part thereof	R20,00
	(ii)	For a copy of an audio record	R30,00

3. The request fee payable by a requester, other than a personal requester, referred to in regulation 11(2) is R50,00.

4. The access fees payable by a requester referred to in regulation 11(3) are as follows:

(1)(a)		For every photocopy of an A4-size page or part thereof	R 1,10
(b)		For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form	R 0,75
(c)		For a copy in a computer-readable form on -	
	(i)	stiffy disc	R 7,50
	(ii)	compact disc	R70,00
(d)	(i)	For a transcription of visual images, for an A4-size page or part thereof	R40,00
	(ii)	For a copy of visual images	R60,00
(e)	(i)	For a transcription of an audio record, for an A4-size page or part thereof	R20,00
	(ii)	For a copy of an audio record	R30,00
(f)		To search for and prepare the record for disclosure, R30,00 for each hour or part of an hour reasonably required for such search and preparation.	

(2) For purposes of section 54(2) of the Act, the following applies:

(a) Six hours as the hours to be exceeded before a deposit is payable; and

(b) one third of the access fee is payable as a deposit by the requester.

(3) The actual postage is payable when a copy of a record must be posted to a requester.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

4.7. Policy: Child Protection Policy

4.7.1. CHILDREN'S PRIVACY

The Company defines Children as individuals under the age of 18. This Processing of Personal Information by the Company is not intended for Children, and we do not intend to collect information about Children. This Company does not knowingly collect information from Children under the age of 18 and we do not target Children under 18 for any marketing purposes. We encourage parents and guardians to take an active role in their Children's online activities and interests.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

SECTION 5: DOCUMENT FLOW, RETENTION AND DESTRUCTION

5.1. Policy: Document Control

5.1.1. PURPOSE

The purpose of this Policy is to ensure that documents containing Personal Information and the security and processing of Personal Information (policies, procedures, data subject forms, and templates, etc.) of the Company are appropriate, up-to-date, and controlled.

This Policy will define the procedure for establishing the controls needed for the identification, storage, protection, retrieval, and retention period of Documents, information, and records (Documents).

This Policy should be read in conjunction with all the Company's Information safety and security policies, as well as the *Acceptable Usage Policy*

5.1.2. INTRODUCTION AND SCOPE`

All Documents are stored electronically and controlled by the Information Officer, who will manage approval, publication, changes, and review, etc. of these documents. There are no controlled paper copy Documents. Once a Document is printed, it is no longer controlled.

5.1.3. APPROVAL

The Information Officer shall be responsible for controlling Documents and for ensuring that Documents are approved prior to issue, by submission to the CEO, and for ensuring that they conform to POPIA requirements.

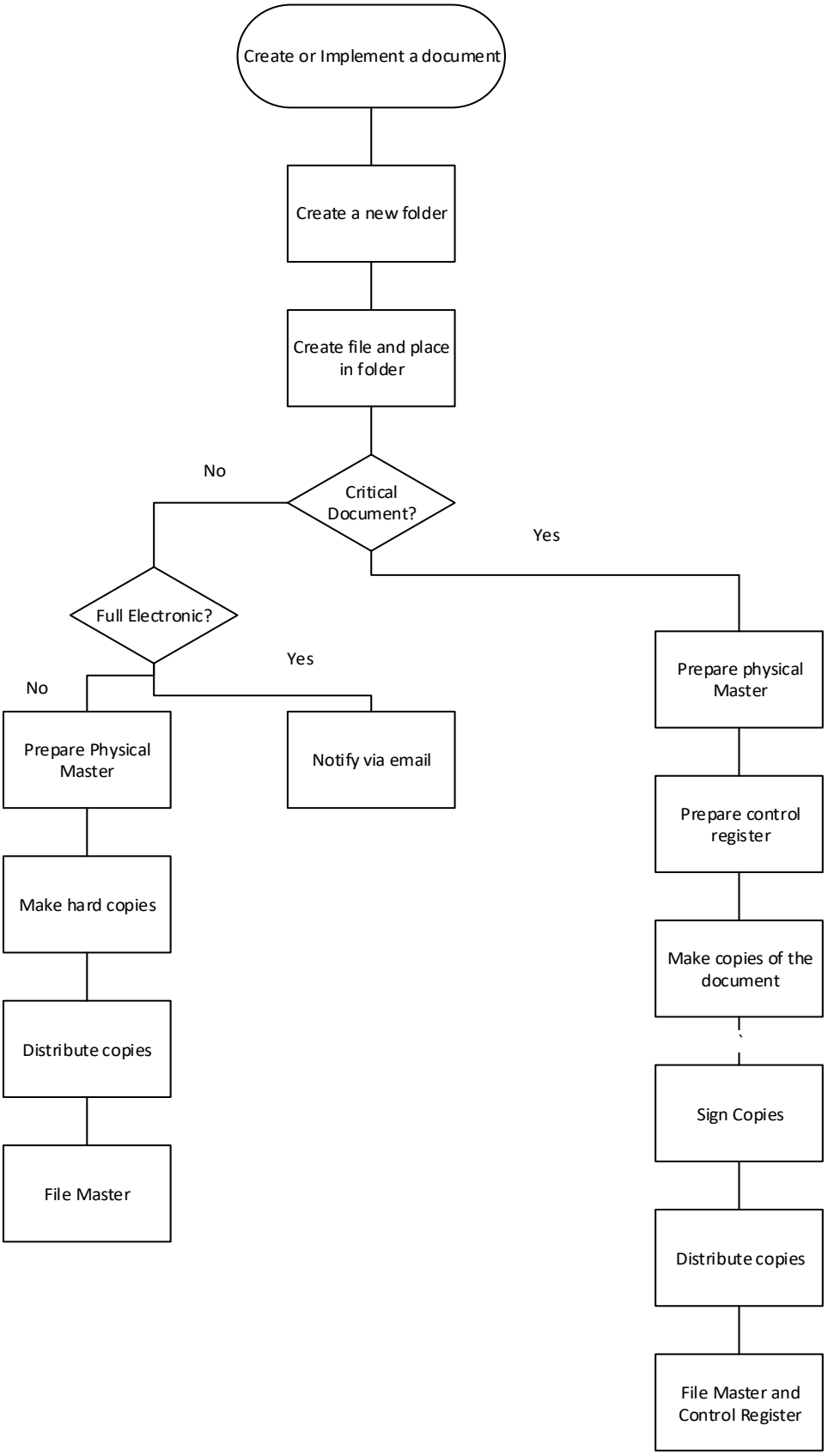
The Information Officer is responsible for receiving all new and revised Documents, and for reviewing Documents.

The CEO will approve all changes to Company Documents.

5.1.4. PROCESS

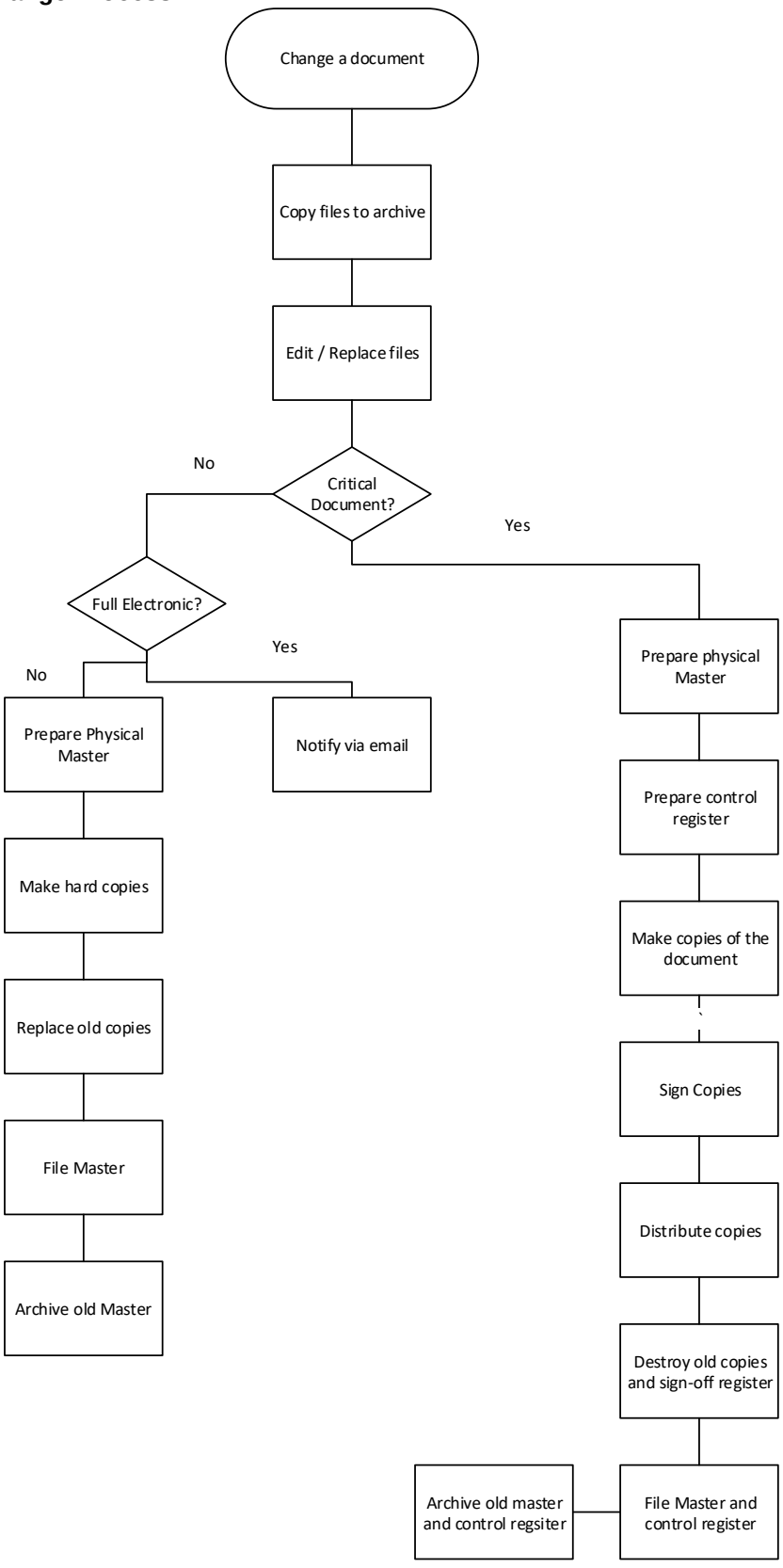
Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Implementation Process



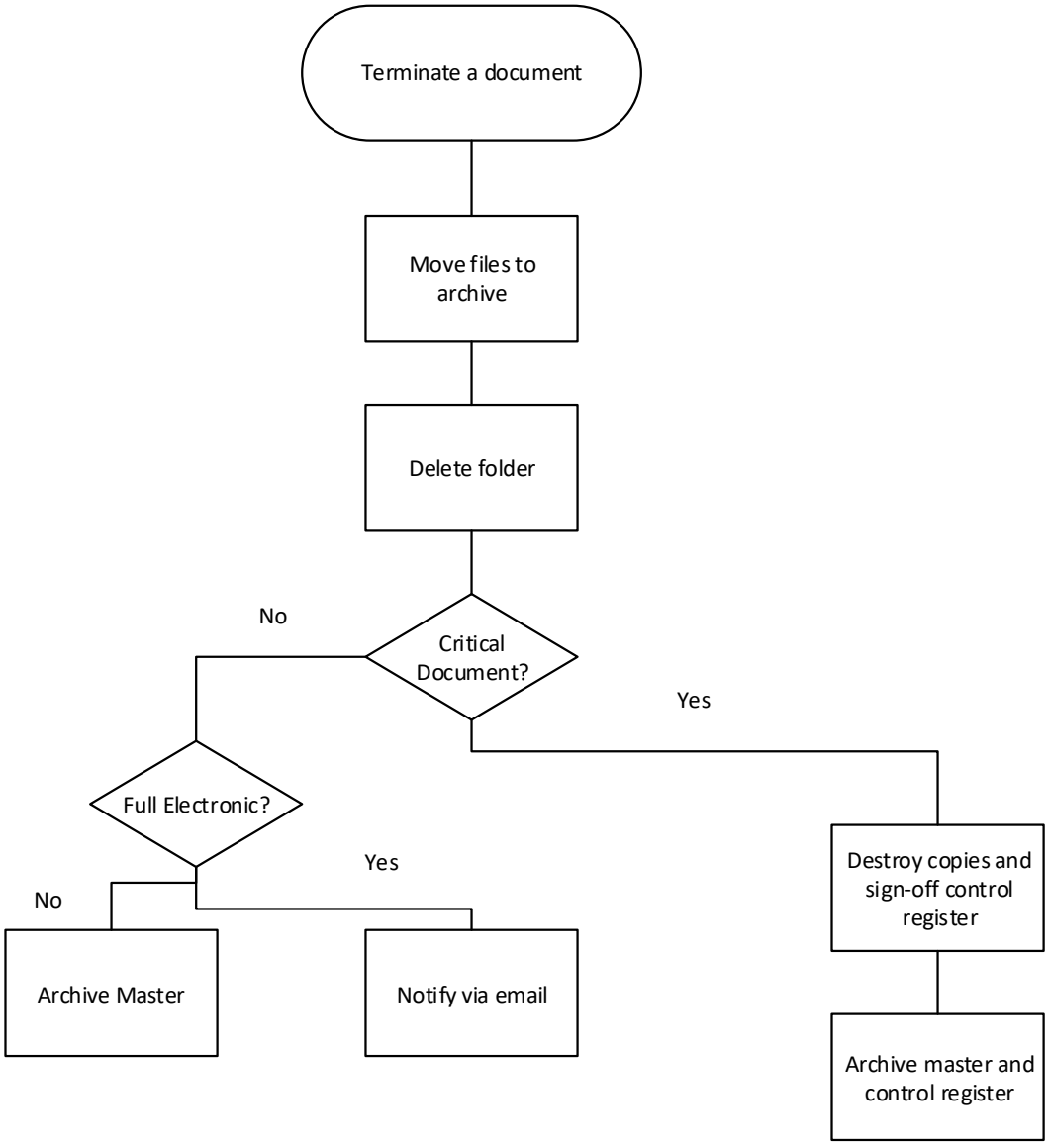
Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Document Change Process



Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Documentation Termination Process



5.1.5. DOCUMENT STATUS, CHANGES, AND DISTRIBUTION

All Documents is kept in a controlled electronic location maintained by the Information Officer. Controlled copies are electronically distributed and may be read by all employees who have access to the system.

Individual documents may be reviewed, updated, and re-approved as often as necessary, whenever applicable legislation or other requirements change, at the discretion of the Information Officer. The whole system and all documents therein will be reviewed a minimum of once annually.

Every time a significant change is made to the Documents, or after 3 minor amendments have accumulated, an Amendment Email is prepared by the Information Officer as the basis for distribution/publication and notifying all employees, Data Subjects (where applicable) and Data Operators.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Uncontrolled Copies

All printed copies of Documents are classed as “uncontrolled”. When documents must be sent electronically, especially to an external organisation or supplier, PDF format should be used, and all applicable security protocols must be followed. Documents containing Personal Information must be password protected and encrypted.

When a Document has been superseded by a later revision, is withdrawn or becomes obsolete, it will be removed from the system to prevent further use. Copies will be retained by the Information Officer. Copies may be retained by others in private and restricted access server locations for reference purposes only, but if so the filename of electronic versions must contain SUPERSEDED or WITHDRAWN or OBSOLETE (likewise hard copies will be physically marked with the appropriate word).

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

5.2. Policy: Information Retention and Destruction

5.2.1. INTRODUCTION

It is important to identify the time periods that Information should be retained by the Company. A retention period is usually the minimum period that Information must be retained. After the retention period has elapsed, such Information must either be archived or destroyed.

It is also important not to retain Information for longer than necessary. Where a retention period has expired, the record in question can be destroyed (*Section 14(1) (a-d) of the Protection of Personal Information Act 4 of 2013*).

5.2.2. OBJECTIVE

The objective of this Policy is to determine the retention period of Information that the Company keeps and describe the process of destruction or archiving such Information.

This Policy applies to all employees, contractors, visitors, Data Operators, and other persons authorised to access and use the Company's systems that create and use Information that relate to the Company's business operations and Data Subjects.

This Policy applies to all records of Information, whether in manual or electronic format.

This Policy should be read in conjunction with other policies of the Company that regulated the protection of Personal Information.

5.2.3. PROCEDURES

Lifecycle of Information

The Company acknowledges that Information has a lifecycle and that, if they have come to an end of their retention period, a decision should be made regarding archiving or destroying them. The Information management lifecycle is as follows:

- The origination of the Information is determined either by the creation of the Information by the Company, or the receipt of the Information by the Company from a compliant third party.
- Once the Information is created or received, it is used, updated, modified, stored, maintained, and protected by the Company on a day-to-day basis.
- At the end of the useful life of the Information in question, or when required by relevant and applicable legislation, the Company must evaluate whether such Information should be archived or destroyed.

Retention of Information

Proper Information management is an important part of doing business and the Company must ensure that it complies with all legislation that is applicable to the Information held by it. As there may be different retention periods depending on the nature of the Information. The guidelines set out below will assist in determining the applicable retention period for Information:

- If a minimum retention period is prescribed by legislation, then the retention period set out in such legislation applies.
- If there is no legislated retention period, the retention period set out in the Company's Policy applies.

- If there is no retention period stipulated in the Policy, or if the Company does not have a Policy, then the retention period prescribed by any specific applicable contract or agreement applies.
- If there is no retention period stipulated in any specific contract or agreement, then any retention period agreed to by the Data Subject in question applies. A Data Subject may agree to records of their Personal Information being held for longer periods of time than that prescribed by legislation or by the Company itself.
- If a Data Subject has not stipulated or consented to a specific retention period in respect of their records of Personal Information, then any retention period prescribed by the CEO applies.
- If none of the above apply, then the Company's Information Officer may determine the applicable retention period.

A table of retention periods are also set out in *Annexure A* for further guidance. Please refer to the *SAICA Guide on The Retention of Records* for more information

Destruction decision

The destruction of Information is not the same as the disposition of Information:

- The disposition of Information refers to the wide range of actions undertaken to manage Information over time, which may include the transfer of Information to an archival storage.
- The destruction of Information is the act of destroying Information permanently by obliterating such Information, so that the Information stored can no longer be physically or electronically reconstructed or recovered. Any decision to destroy Information must be formally approved by the CEO and Information Officer in writing.

Where the retention period for Information has expired, a decision must be made to either:

- Continue to retain the document (if permitted by law).
- Transfer the Information to an archival storage.
- Destroy the Information.

Some of the factors that will influence this decision are:

- If the Information reached its useful life.
- Could there be a future challenge where the Information is needed in a civil or criminal case?
- Does the Information need to be retained for commercial or business purposes?

The abovementioned decision must be formally made and must be properly documented. Such decision must be in writing and must be signed off by the CEO and the Information Officer.

Destruction of paper records

Where a formal decision has been made to destroy Company Information, the destruction must be done securely. Paper records must either be shredded by the Company or placed in confidential bins to be removed for shredding by a reputable third-party provider.

Paper records must not be discarded in trash cans or destroyed by other unsecured methods.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Destruction of electronic Information

Before electronic Information is destroyed, archiving the Information should be considered. If the decision is made to destroy the Information, then one of the following techniques must be used:

- Overwriting: Overwriting is an effective method of destroying electronic Information. This method involves the use of software that overwrites the record multiple times. This makes the possibility of recovering the Information much more remote.
- **Physically destroying storage media**: Physically destroying the storage media or record must be used where Personal Information, and sensitive or confidential Information of the Company is stored. This is also the most appropriate method of destroying Information stored on portable media, such as hard drives, and shredding CDs and DVDs.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (5.2) A: RETENTION PERIOD OF INFORMATION

Document / Record / Information	Retention period (years)
Acceptance forms	12
Accident book and records	7
Accounting records of stock of brokers and carrier against shares	5
Accounts payable ledgers and schedules	7
Action Plans / Requests	5
Agreements after termination	5
Agreements with architects and builders (after day of completion)	5
Allotment letters	12
Allotment sheets and return of allotment	15
Annual Financial Statements	15
Annual return and supporting documents	15
Application for jobs – unsuccessful	1
Application forms	12
Apprentice records of remuneration	3
Arbitration award records	3
Aspects and Impacts Register	Continuous
Audit Reports	Permanently
Bank Reconciliations	2
Bank statements, deposit slips, stock lists paid by its member	4 years from last date of entry
Books of account	15
Calibration Records	5
Cancelled share of debenture certificates and balance receipts (many large transfer offices keep for one year only)	3

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Cancelled share transfer forms	12
Cash books	15
Certificates and documents of title	Permanently or until sold
Change of address – notification	1
Checks (for important payments and purchases)	Permanently
Collective Agreement records	3
Contract Reviews	5
Contracts and leases (expired)	7
Contracts and leases (still in effect)	Permanently
Correspondence (general)	2
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2
Costing Records	5
Creditor’s invoices and statements	5
Customer Complaints	5
Customer Sign-off/Proof of Delivery	5
Customer Specifications	5
Debtor’s statements	4
Deeds of Title	Permanently or until disposed
Delivery Notes/Advice Notes	5
Deposit slips	4
Depreciation Schedules	Permanently
Detailed records of the registered vendor’s transactions	4 years from last date of entry
Determination records made in respect of the Wage Act	3
Dispute records	3
Dividends and interest	15

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Documents of incorporation including: • Certificate of change of name • Certificate of incorporation • Certificate to commence business	Permanently
Duplicate deposit slips	2
Employee Training records and certificates	5 years after service terminated.
Employment applications	3
Employment Equity Plan	3 years after expiry date
Evaluation of legal and Other Requirements	Continuous
Expense accounts	4
Expense Analyses / expense distribution schedules	7
Financial Statements (year-end)	Permanently
Fixed asset register	15
General ledgers	15
Goods received notes	4
Incidents reported at work	3
Income tax required records	4
Indemnities and guarantees	5 years after date of expiry
Index of members	15
Inspection and Test Records	5
Insurance Policies	5
Insurance Policies (expired)	3 years
Insurance records, current accident reports, claims, policies and the like	Permanently
Internal audit reports	3
Invoices (to customers, from vendors)	7
Leases (after date of expiry of lease and all queries have been settled)	5

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Letter of Good Standing with Compensation Commissioner	3 years after expiry date
Letters of indemnity for lost share certificates	Permanently
Licensing agreements	5 years after date of expiry
Maintenance Records	5
Management Reviews	5
Memorandum and Articles of Association	Permanently
Method Statements & Drawings	5
Minute books, bylaws, and charter	Permanently
Minutes of Health and Safety Committee meetings	3
Minutes of meetings (originals for): • Board meetings • Committee meetings • General meetings	Permanently
NCI (Nonconformity, Corrective/Preventive Action, Improvement) reports	5
Obsolete personal data	Destroy
Payroll records and summaries	7
Payrolls	7
Personal information and purpose for which data was collected must be kept by the person who electronically requests, collects, collates, processes, and stores the information.	As long as the information is used plus 1 year.
Personal records of organisation's executives	Permanently
Personnel files (terminated employees)	7
Petty Cash books	15
Power of attorney, stop notices and similar court orders (from date person ceased to be a member)	15
Purchase invoices	4
Purchase orders	4

Purchase Specification / Orders	5
Receipts	4
Records of strike, lock-out or protest action	Permanently
Records of subscriptions or levies paid by its members	15
Records of third parties to whom the information was disclosed.	As long as the information is used plus 1 year.
Redemption / conversion discharge forms of endorsed certificates	12
Register of debenture holders	15
Register of directors and officers	15
Register of directors' interest on contracts	15
Retirement records	Permanently
Salary revision schedules	7
Salary wage register	7
Sales invoices	4
Sectional title records	Permanently
Share investment certificates	Permanently or until sold
Staff records (after date employment ceased)	7
Subcontractor Records	5
System Audit Reports	5
Tax return - employees	4
Tax returns and worksheets	Permanently
Taxation returns and assessments	15
Time and piecework records	7
Trademark registrations and copyrights	Permanently
Transfer duty records	Permanently
Unemployment insurance	Until service terminated

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Wage and salary records (including overtime)	7
Waste Transfer Notes	3
Withholding tax statements	7
Workmen’s Compensation records	3

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

SECTION 6: INCIDENT MANAGEMENT AND REPORTING

6.1. Policy: Information Incident Management Process

6.1.1. PURPOSE

This Policy was developed to provide direction to guide all employees, contractors, visitors, Data Operators, and other persons authorised to access and use the systems of the Company, on how to respond to incidents that threaten the security of Personal Information.

The purpose of this Policy is to:

- Provide a framework for responding to Information Incidents (including data breaches) in accordance with POPIA.
- Assist the Users in understanding their responsibilities in addressing and dealing with Information Incidents.

This Policy applies to all Users, and any person handling information or data processed by the Company.

This Policy should be read in conjunction with other policies of the Company that regulate the protection of Personal Information.

6.1.2. POLICY

The incident management of an Information Incident is vital to the Company. By handling such incidents correctly, the impact on the reputation of the Company, and other damage to the Company can be managed. Implementing the necessary control measures in the case of an information or data breach is critical.

6.1.3. INFORMATION INCIDENTS

This section of the Policy sets out the steps that must be taken in response to an Information Incident in relation to the Company, including the roles and responsibilities of all stakeholders involved.

An Information Incident means a single or a series of unwanted or unexpected events that threaten information security or privacy. Information Incidents include any collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorised by the Company.

Information Incidents include Privacy Breaches, which are unauthorised collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alteration, consultation, use or dissemination by means of transmission, merging, linking, disposal (erasure or destruction), or storage of Personal Information, whether accidental or deliberate. If these breaches include Personal Information, POPIA will be applicable to both Information Incidents and Privacy Breaches.

6.1.4. INFORMATION OFFICER

The Information Officer of the Company is responsible for the coordination, investigation, and resolution of all Information Incidents.

The Information Officer will be responsible for determining when a decision must be made to either notify or not notify Data Subjects of an Information Incident based on a balance of harms or as required by relevant legislation, including POPIA (*Refer to Annexure B and Annexure C*).

The Information Officer is solely responsible for liaising with the Information Regulator regarding an actual or suspected Privacy Breach or Information Incident.

6.1.5. PROCESS: INFORMATION INCIDENT REPORTING

Any User or other person who discovers a suspected or actual Information Incident, including a Privacy Breach, must immediately report it to their supervisor and or manager. The supervisor or manager must then report it to the Information Officer immediately (*Refer to Annexure A*). The Information Incident must then be recorded in an Incident Register (*Refer to Annexure D and Annexure E*).

In circumstances where the supervisor or management contact is not immediately available, whether in person or by phone, the User must immediately report the Information Incident directly to the Information Officer.

Where the Information Incident will have serious impact on the Company, the Information Officer must request the User reporting the Information Incident to:

- Assess and document the Information Incident including, the nature, sensitivity, volume, impact, and type of Incident in question (*Refer to Annexure D, E and F*).
- Assist with resolving the Information Incident or containing the Information Incident.
- Provide the User reporting the Information Incident with instructions regarding how to deal with the Information Incident response, such as:
    - Containing the loss.
    - Preventing a recurrence.
    - Determining the next steps.

The Information Officer must decide if additional information should be gathered to determine the response strategy to the Information Incident, including the (*Refer to Annexure D, E and F*):

- Type of Information Incident.
- Nature and sensitivity of the Information Incident.
- Volume.
- Impact and implications of unauthorised disclosures or asset losses.

The Information Officer determines whether the Information Incident is major or minor, based on the following:

- The Information Incident involves Personal Information, sensitive, confidential, proprietary, or critical information of the Company.
- If there is a reasonable expectation of harm to any data subject because of the Information Incident.
- Whether data subjects will be, notified that their Personal Information has been compromised.
- Whether the incident will be reported to the Information Regulator.
- Whether the Information Incident has a serious or potentially serious public impact.

Minor Information Incidents:

- The User in question will be the main point of contact for the breach in question.
- The User will refer all minor Information Incidents to the Information Officer for follow-up and resolution in collaboration with CEO of the Company.

- The Information Officer must request the User to provide a report regarding the Information Incident.

Major Information Incidents:

- The Information Officer must coordinate an Incident Management and Investigation Process to conduct an assessment and gather evidence regarding the Information Incident.

6.1.6. NOTIFICATION OF THE REGULATOR

The Information Officer will determine if there was a breach of any Data Subject's Personal Information, and whether such breach should be reported to the Regulator (*Refer to Annexure D, E and F*). The following factors need to be considered before reporting any Information Incident to the Regulator:

- The nature of the Information Incident in question.
- The legitimate needs of law enforcement to act on the Information Incident.
- Measures that are reasonably necessary to determine the scope and extent of the compromise.
- Measures that should be taken to restore the integrity of the Company's information systems.

The Information Officer must ensure that any breach or compromise is reported to the Regulator as soon as reasonably possible after the discovery of the compromise (*Section 22 of POPIA*), if determined, as necessary.

6.1.7. NOTIFICATION OF DATA SUBJECTS

The impact of Privacy Breaches must be reviewed to determine if it is appropriate to notify individual Data Subjects whose Personal Information has been affected. The User will work with the Information Officer to notify affected parties and take other required action that may be appropriate in the circumstances (*Refer to Annexure B and C*).

The key consideration in deciding whether to notify an affected individual is whether such notification is necessary to avoid harm to an individual, such as:

- Identity theft or fraud.
- Physical harm.
- Damage to reputation.
- Business or employment opportunities.

Other considerations in determining whether to notify individual data subjects include the following:

- Any legislative requirements for notification such as required by Section 22 of POPIA.
- Any contractual obligations that may require notification.
- A risk of loss of confidence in the Company.
- Good customer relations dictate that notification is appropriate.

Notification is determined by the *balance of harms*. Under this principle, an individual Data Subject who could potentially face harm because of an Information Incident may not be notified if it is determined that the harm that would result from a notification would outweigh the benefit to be gained from the notification.

If it is determined that notification of individual Data Subjects would be appropriate in the circumstances of an Information Incident, the:

- Notification should occur as soon as possible following the breach.
- All affected individuals should be notified directly.

6.1.8. CLOSURE OF INFORMATION INCIDENT FILE

When closing an Information Incident file, the Information Officer must notify the CEO. The Information Officer will also write a final report (*Refer to Annexure F*), including recommendations, and submit it to all stakeholders. There are 2 types of recommendations included in the Report, namely:

- Essential recommendations, which must be implemented promptly.
- Advisory recommendations, which the CEO will decide whether to implement.

6.1.9. COMPLIANCE

The Information Officer will be responsible for implementing the recommendations set out in the Report. The Information Officer may perform compliance reviews or may audit the implementation of the recommendations set out in the Report and their effectiveness once implemented.

6.1.10. RESPONSIBILITIES

User

In the case of any actual or suspected Information Incident, the User's responsibilities are to:

- Report the Information Incident immediately to the Information Officer or their manager.
- Recover the Personal Information or Confidential Information, if possible,
- Contain the Information Incident to lessen its impact and implication for the Company and the Data Subjects involved.
- Remediate the Information Incident by working with the Information Officer to determine the specifics of the Information Incident to resolve it.
- Prevent Information Incidents by being diligent in the handling of Personal Information, and Confidential Information.
- Be an active participant in developing the culture of prudent information management.

Contractor or Service Provider (Data Operator):

Where the User in question is a Data Operator, in the case of an Information Incident, the Data Operator's responsibilities are to:

- Ensure that their employees, service providers, or any other persons who discover an Information Incident (including a Privacy Breach) immediately notify the management of such Data Operator, who must then report it to the Information Officer of the Company.
- Ensure that the Information Incident is immediately recorded in the Register (*Refer to Annexure D and E)*.
- Recover the Personal Information or Confidential Information, if possible.
- Contain the incident to lessen the impact for the Company and any Data Subjects.
- Remediate the Information Incident.
- Work collaboratively with the Information Officer.
- Support the investigation and Information Officer.
- Notify any Data Subjects (whether individuals or juristic persons) affected by the Information Incident, as directed by the Information Officer.
- Prevent Information Incidents by:
    - Ensuring that employees know and understand how to apply changes in the handling of Personal Information, and Confidential Information.
    - Being diligent in the handling of Personal Information and Confidential Information.
    - Implementing recommendations from the Information Incident reporting process and the Information Officer.
    - Developing a culture for the prudent management of information within the Data Operator's business.
    - Providing training.

- Ensuring that their employees understand their responsibility in reporting Information Incidents, including containing the loss and recovering the information.

The Information Officer:

The Information Officer's responsibilities in respect of any Information Incident are to:

- Receive the report about the Information Incident from the User and provide direction on assessing the Information Incident.
- Ensuring its recorded in the Register (*Refer to Annexure D and E)*.
- Determine if the Personal Information, or Confidential Information in question can be recovered.
- If the loss or disclosure can otherwise be contained.
- The coordination, investigation, and resolution of all Information Incidents, including Privacy Breaches.
- Receive and review status reports and compile the Report and present to the CEO the implementation of the recommendations contained in the Report.
- Ensure that the recommended controls in the Report are implemented.
- Report Information Incidents to the CEO (*Refer to Annexure D and E)*.
- Contact all responsible stakeholders to ensure communication, recommendation, and collaboration.
- Liaise with the Information Regulator on Privacy Breaches and other Information Incidents.

The Information Officer must prevent Information Incidents by:

- Implementing the recommendations set out in the Report.
- Ensuring that Users know and understand how to apply changes in the handling of Personal Information, and Confidential Information.
- Participating in the development of a culture within the Company for the prudent management of information.
- Providing appropriate training.
- Ensuring that Users understand their responsibility in reporting all Information Incidents, including the importance of containing the loss and recovering the information.
- Notifying any Data Subjects (both individuals and juristic entities) affected by the Information Incident.
- Ensuring that Data Operators understand their responsibilities in the Information Incident reporting process and collaborating with them to ensure timely and accurate reporting.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) A: POPIA INCIDENT / EVENT NOTIFICATION TO INFORMATION OFFICER

User Full Name:	
User Designation:	
User Department (*if applicable):*	
User Email Address:	
User Contact Nr:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

Information Incident Description:

Description of Incident / Event:	
How did it happen?	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Who caused it?	
What was the impact or damage?	
What was the loss?	
When did it happen?	
How can it be prevented from happening again?	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) B: DATA BREACH NOTIFICATION PROCESS

(*To be placed on your website*)

Name of Information Officer:	
Email Address of Information Officer:	
Date:	

INTRODUCTION

The POPI Act aims to protect the rights of individuals about whom data is obtained, stored, processed, or supplied. POPIA requires that the Company takes appropriate security measures against unauthorised access, alteration, disclosure or destruction of Personal Information and data.

The POPIA places obligations on employees to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All employees are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all employees to enable them to carry out their obligations within this Process.

Data Operators will be provided with a copy of this Process and will be required to notify the Company of any data breach without delay after becoming aware of the data breach. Failure to do so may result in termination of the Processing Agreement.

Breach of this Process will be treated as a disciplinary offence which may result in disciplinary action, including summary dismissal depending on the seriousness of the breach.

Changes to data protection legislation will be monitored and amendments may be required to this Process to remain compliant with legal obligations.

RESPONSIBILITY

The Information Officer has overall responsibility for breach notification within the Company.

The Information Officer is responsible for ensuring Breach Notification Processes are adhered to by all employees and are the designated point of contact for personal data breaches.

The Information Officer is responsible for overseeing this Process and developing data-related Policies and Guidelines.

Please contact the Information Officer with any questions about this Process or the POPI Act, or if you have any concerns that this Process has not been followed.

The Information Officer’s contact details are set at the start of this document.

A PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information or Special Category Information transmitted, stored, or otherwise processed.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Examples of a data breach could include the following:

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (for example sending an e-mail or SMS to the wrong recipient).
- Unforeseen circumstances such as a fire or flood.
- Hacking, phishing, and other attacks where Information is obtained by deceiving whoever holds it.

REPORTING A DATA BREACH

The Company must notify the Information Officer of a data breach where it is likely to result in a risk to the rights and freedoms of individuals.

Examples of where the breach may have a significant effect includes:

- Potential or actual discrimination.
- Potential or actual financial loss.
- Potential or actual loss of confidentiality.
- Risk to physical safety or reputation.
- Exposure to identity theft.
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

MANAGING AND RECORDING THE BREACH

On being notified of personal data breach, the Information Officer will take immediate steps to establish whether a personal data breach has in fact occurred. If so, the Information Officer will take steps to:

- Where possible, contain the data breach.
- As far as possible, recover, rectify, or delete the data that has been lost, damaged, or disclosed.
- Assess and record the breach in the Company' Register.
- Notify the Information Regulator.
- Notify data subjects affected by the breach.
- Notify other appropriate parties to the breach.
- Take steps to prevent future breaches.

NOTIFYING THE INFORMATION REGULATOR

The Information Officer will notify the Information Regulator when a personal data breach has occurred, which is likely to result in a risk to the rights and freedoms of individuals.

This will be done, where possible, within 72 hours of becoming aware of the breach. If the Company is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the Information Regulator.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

NOTIFYING DATA SUBJECTS

Where the data breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the Information Officer will notify the affected individuals, the likely consequences of the data breach and the measures the Company intends to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Management will cooperate with and seek guidance from the Information Officer, the Information Regulator, and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the Data Subjects directly (for example, by not having contact details of the affected individuals) then the Company will consider alternative means to make those affected aware, for example, by making a statement on the Company's website.

ASSESSING THE BREACH

Once initial reporting procedures have been carried out, the Company will carry out all necessary investigations into the breach.

The Company will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction, or unauthorised disclosure of personal data. The Company will identify ways to recover correct or delete data, for example notifying our insurers or the police if the breach involves stolen hardware or data.

Having dealt with containing the breach, the Company will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken, for example notifying the Information Regulator or Data Subjects.

These factors include:

- What type of data is involved and how sensitive it is?
- The volume of data affected.
- Who is affected by the breach?
- The consequences of the breach on Data Subjects and whether further issues are likely to materialise?
- Are there any protections in place to secure the data?
- What has happened to the data?
- What could the data tell a third-party about the Data Subject?
- What are the likely consequences of the personal data breach on the Company?
- Any other consequences which may be applicable.

PREVENTING FUTURE BREACHES

Once the data breach has been dealt with, the Company will consider its security processes with the aim of preventing further breaches. To do this, the Company will:

- Establish what security measures were in place when the breach occurred.
- Assess if technical or organisational measures can be implemented to prevent the breach happening again.
- Consider if there is adequate employee awareness of security issues.
- Consider whether it is necessary to conduct a privacy or data protection impact assessment.
- Consider whether further audits or data protection steps need to be taken.
- To update the Information Incident Register.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

REPORTING DATA PROTECTION CONCERNS

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time, and we would encourage you to report any concerns that you may have, to the Information Officer.

REPORTING A DATA BREACH

If you know or suspect a personal data breach has occurred or may occur, you should:

- Complete a POPIA Incident / Event Notification Form, which can be obtained from the Information Officer.
- Email the completed form to the Information Officer.

Breach reporting is encouraged throughout the Company and employees are expected to seek advice from the Information Officer, if they are unsure as to whether the breach should be reported and could result in a risk to the rights and freedom of individuals.

Once reported, you should not take any further action in relation to the breach. The Information Officer will acknowledge receipt of the POPIA Incident / Event Notification Form and take appropriate steps to deal with the report.

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) C: NOTIFICATION OF SECURITY BREACH IN TERMS OF SECTION 22 OF POPI ACT

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

TO THE DATA SUBJECT:

Full Name:	
ID Number:	
Email Address:	

TO THE INFORMATION REGULATOR:

Official Full Name:	
Contact Number:	
Email Address:	

INCIDENT DESCRIPTION (INFORMATION TO BE SUPPLIED IN TERMS OF POPIA SECTION 22)

Description of security breach and compromise of Personal Information of a Data Subject	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Consequences of the security breach	
Measures to be taken by the Company to address and rectify the security breach.	
Measures taken by Data Subject to mitigate the adverse effects of the data breach or compromise.	
Identity of person who caused the security breach or compromise.	

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) D: DATA BREACH NOTIFICATION REGISTER

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

DATE REPORTED	REPORTED BY WHOM	DATA SUBJECT NAME	INCIDENT / EVENT	STEPS TAKEN TO REMEDY BREACH

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) E: POPIA REGISTER REPORT

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

PERSONAL INFORMATION RECORD / FORM	DATA SUBJECT NAME	POPIA INCIDENTS AND BREACHES IDENTIFICATION	HOW INCIDENTS / BREACHES ARE MITIGATED	OUTSTANDING POPIA CONTROLS REQUIRED

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) F: POPIA COMPLIANCE REPORT

Company Name:	
Company Registration Number:	
VAT Registration Number (*if applicable):*	
Physical Address:	
Name of Information Officer:	
Email Address of Information Officer:	
Date:	

KEY POPIA COMPLIANCE AREAS	YES	NO	COMMENT/ACTION
POPIA POLICIES			
The following POPIA Policies are in place:			
The following POPIA Policies are outstanding:			

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

POPIA PROCEDURES			
The following POPIA Procedures and Controls are in place:			
The following POPIA Procedures and Controls are outstanding:			

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

POPIA BREACHES			
The following POPIA Breaches have been reported during the year under review. If not resolved, indicate in comment section.			
KEY POPIA COMPLIANCE AREAS	**YES**	**NO**	**COMMENT/ACTION**
POPIA RISK REGISTER			
The Top 10 POPIA Risks are as follows. If not mitigated, indicate in Comment Section:			

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

POPIA REGISTER			
The following POPIA Registers are in place:			
New POPIA Registers to be issued:			
POPIA REPORTS:			
The following POPIA Reports are in place			
New POPIA Reports to be issued:			

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) G: DATA SUBJECT DISAGREEMENT REGARDING MICROSOFT PERSONAL DATA

The following information will be maintained by Akili when there is disagreement regarding Microsoft Personal data

Name of the Data Subject:	
Contact Information of subject:	
Unique Identifier of subject:	
Date of Complaint/Dispute Raised:	
Nature of Dispute:	
Summary of data incident:	
Date of Escalation to Microsoft:	
Details of Escalation:	
Microsoft Response:	
Corrective Actions Implemented:	
Date of Resolution:	
Status of the Complaint:	

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) H: NOTIFY MICROSOFT

Microsoft will be notified using SupplierWeb or email SuppIR@microsoft.com in case of any incident involving Microsoft Personal data. The following information will be sent to Microsoft

Data incident Date:	
Supplier name:	
Supplier number:	
Date of Complaint/Dispute Raised:	
Microsoft contacts notified:	
Associate PO, if available/applicable	
Summary of the data incident:	

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	

Company Name:	Akili IT Services (Pty) Ltd
Company Reg Nr:	2018/603685/07
Date:	20/11/2024

ANNEXURE (6.1) I: ACCESS TO DATA SUBJECT RECORDS

The below data is maintained with respect to Data Subject requests related to Microsoft Personal data

Data and time of request:	
Type of request: (Access, Deletion, rectification)	
Name and contact of Data subject:	
Action taken by supplier:	
Specific data that was Accessed, modified or deleted:	
Reason for denying access/deletion/modification request:	
Status of request:	

Signed at _____ on this _____day of _____ 20_____

Information Officer Name:	
Signature:	