SECTION 51 MANUAL

In terms of the Promotion to Access to Information Act no 2 of 2000 (as amended)

wireless • fibre • voice • data

WIRULINK PROPRIETARY LIMITED
Registered Name
("the company")

2006/011482/07
Registration Number

JB MAREE
CHIEF EXECUTIVE OFFICER

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1.	"CEO"	Chief Executive Officer;
1.2.	"DIO"	Deputy Information Officer;
1.3.	"IO"	Information Officer;
1.4.	"Minister"	Minister of Justice and Correctional Services;
1.5.	"PAIA"	Promotion of Access to Information Act No. 2 of 2000 (as amended);
1.6.	"POPIA"	Protection of Personal Information Act No. 4 of 2013;
1.7.	"Regulator"	The Information Regulator;
1.8.	"Republic"	Republic of South Africa

2. THE MANUAL

2.1. Objectives of the Act

The Promotion of Access to Information Act, 2 of 2000 ("the Act") (as amended), which came into effect on the 9th of March 2001, seeks to advance the values of transparency and accountability in South Africa. Aligned with the Protection of Personal Information Act, 4 of 2013 (POPIA).

The 1996 South African Constitution by providing a statutory right of access on request to any record held by the state as well as access to records held by private bodies entrenches the fundamental right to information.
The Act establishes the following statutory rights of requestors to any record of a private body if the following circumstances are met:

- if the record is required for the exercise or protection of any of his or her legal rights;
- the requestor complies with all the procedural requirements; and
- the access is not refused in terms of any ground referred to in the Act.

Section 51 of the Act obliges private bodies to compile a Manual. The purpose of the manual is to assist an individual to obtain access to the records of a private body and the Act stipulates the minimum requirements with which a manual has to comply.

2.2. Scope of the Manual

This manual ("Manual") has been prepared by the company and applies to all of the private bodies. This Manual is prepared in accordance with Section 51 of PAIA and incorporates requirements of POPIA. It is published in accordance with the requirements of section 51 of the Act and is aimed at facilitating access to records held by the company in terms of the Act. It provides guidance on accessing records and how personal information is processed.
Specifically, the Manual provides information on:

- the contact details of the information officer, who will deal with a person's request;
- the main business of the company;
- the subjects and categories of records that are held by the company;
- records that are automatically available, without a person having to request access;
- records that are available in terms of any other legislation; and
- the procedure that needs to be followed to obtain access to a record.

2.3. Availability of the Manual

2.3.1. A copy of the Manual is available:

2.3.1.1. on website: www.wiru.co.za

2.3.1.2. By e-mail: paia@wiru.co.za

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

2.3.1.4. to the Information Regulator upon request.

2.3.2. A fee for a copy of the Manual, as contemplated in Annexure B of the Regulations, shall be payable per each A4-size photocopy made.

3. COMPANY DETAILS

3.1. The Company is a private company incorporated in terms of the Company laws of the Republic Of South Africa.

3.2. The main business of The Company is : General trading in the communications industry and all business related thereto.

3.3. The Company has no subsidiaries.

3.4. The Company employs approximately 54 permanent staff members.

3.5. The Company is registered as a member with a controlling body, The Independent Communications Authority of South Africa (ICASA).

4. COMPANY INFORMATION OFFICER OF WIRUlink PTY LTD

The Information Office shall ensure that the requirements of the Act are administered in a fair, objective and unbiased manner:

4.1. Information Officer

Name:	Shirell Maree
Business address:	Unit 44, 7th Floor, 114 West Street, Sandton, 2196, Gauteng, South Africa
Tel:	+27 010 595 0000
E-mail:	shirell@wiru.co.za

4.2. Deputy Information Officer

Name:	Adriaan Petrus Maree
Business address:	Unit 44, 7th Floor, 114 West Street, Sandton, 2196, Gauteng, South Africa
Tel:	+27 010 595 0000
E-mail:	paia@wiru.co.za

5. ENTRY POINTS FOR REQUESTS

The CEO of the Company has delegated his/her powers in terms of the Act to the Information Officer, who will handle all requests in terms of this Act on his/her behalf. All requests in terms of the Act must be addressed to the Information Office with details given in clause 4 above.

6. WHO MAY REQUEST ACCESS TO INFORMATION

The Act provides that a person may only request information in terms of the Act if the information is required for the protection of a right. Only requests for access, where the requestor can furnish the Information Officer with sufficient particulars as to the right the requestor is seeking to protect, will be considered.

A requestor can request access to information in different capacities. The category under which the request falls will influence the amount to be charged when a request is lodged.

Requestors can be classified in accordance with the following different categories:

- a personal requestor, that is a person who requests information about him / herself;
- an agent requestor, that is a person requesting information on behalf of someone else;
- a third party requestor, that is a person requesting information about someone else; or
- a public body, requests information in the public interest

7. GUIDANCE TO REQUESTORS

7.1. The Information Regulator has, in terms of Section 10 (1) of the Act, as amended, updated and made available the revised Guide ("the Guide"), as may reasonably be required by a person who wishes to exercise any right contemplated in the Act.

7.2. The Guide is available in each of the official languages.

7.3. The Guide will include the following:

- a description of the objectives of the Act;
- the relevant information of every private body as applicable;
- the manner and form in which requests must be lodged;
- the remedies available to requestors should a body not comply with the Act;
- the manner in which an appeal can be lodged;
- the fees payable in relation to requests for access; and
- a reference to any regulations passed.

7.4. Members of the Public can inspect or make copies of the Guide from the offices of the Regulator, during normal working hours.

7.5. The Guide can also be obtained:

7.5.1. Upon request to the Information Officer;

7.5.2. From the website of the Regulator https://inforegulator.org.za/paia/

7.5.3. This guide and additional information may be requested from the Regulator enquiries@inforegulator.org.za

8. RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION

8.1. Unlimited requestors

The following information is available without special request. Records that are kept automatically available to the public are records of the Company lodged in terms of government requirements with various statutory bodies, including the Registrar of Companies, and the Registrar of Deeds, all records in the marketing and advertising material published by the company and all records available on the company's website.

8.2. Limited requestors

Certain legislation mandates private bodies to allow certain person(s) access to specified information, upon request. Legislation that may be consulted to establish the type of information or record and the person(s) having access thereto is as follows:

- Basic Conditions of Employment Act 75 of 1997;
- Broadcasting Act of 1999;
- Business Act of 1991;
- Occupational Health and Safety Act 85 of 1993;
- Companies Act 61 of 1973;
- Companies Act 71 of 2008;
- Competition Act 12 of 2010;
- Compensation for Occupational Injuries & Diseases Act 130 of 1993;
- Consumer Protection Act 68 of 2008;
- Electronic Communications Act of 2005
- Electronic Communications and Transactions Act 25 of 2002;
- Employment Equity Act 55 of 1998;
- Income Tax Act 58 0f 1962;
- Independent Communications Authority of South Africa Act of 2000
- Labour Relations Act 66 of 1995;
- National Credit Act 34 of 2005;
- Protection of Businesses Act of 1978;
- Protection of Personal Information Act of 2013
- Protected Disclosure Act 26 of 2000;
- Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002;
- South African Revenue Services Act of 1997;
- Skills Development Act 97 of 1998;
- Unemployment Contributions Act No 4 of 2002;
- Unemployment Insurance Act 63 of 2001;
- Value Added Tax Act 12 of 2011;

9. PROCEDURE

9.1. Prescribed access form

In order for us to facilitate your access to a record, you need to complete the prescribed access form. Please take note that the prescribed access form must be completed in full and that failure to do so may result in the process being delayed until such additional information is provided. Prescribed PAIA request forms are available on the Information Regulator website https://inforegulator.org.za/paia/

9.2. Proof of Identity

Proof of identity is required to authenticate the request and the requestor. Therefore in addition to the access form, requestors will be required to supply a certified copy of their identification document or any other legally acceptable means of identification.

9.3. Prescribed fees

Please take note that a request will not be processed until the request fee and/or the deposit (if applicable) have been paid. Requestors are advised that four types of fees are provided for in terms of the Act.

The fee structure can be obtained from the Regulator website: https://inforegulator.org.za/paia-fees-structure-2/

9.3.1. Reproduction fee: this fee is payable with respect to all records that are automatically available;

9.3.2. Request fee: this fee is an administration fee that must be paid by all requestors, except personal requestors (a personal requestor is a requestor seeking access containing information about the requestor himself/herself), before the request is considered and is not refundable;

9.3.3. Access fee: which is payable once access to a record is granted, this fee is intended to re-imburse the company for the costs involved in searching and preparing the record for delivery;

9.3.4. Deposit: which is payable if the company receives a request for access to information about a person other than the requestor himself/herself and where the preparation of the record will take longer than six hours.

10. GRANTING OR REFUSAL OF REQUESTS

All requests that meet the requirements, as set out above will be processed in accordance with the time limits as set out in the Act.

Requestors should take note that requests may be refused based on the following grounds, as set out in the Act:

- mandatory protection of privacy of a third party who is a natural person;
- mandatory protection of commercial information of a third party;
- mandatory protection of certain confidential information of a third party;
- mandatory protection of records privileged from production in legal proceedings;
- commercial information of the private body; and
- mandatory protection of research information of a third party and of the private body.

Requestors will be informed within 30 days of a decision to refuse access to the information requested on one of the above grounds. Please take note that in terms of the Act, the 30 day period maybe extended for a further 30 day period should more time be required to gather the requested information. The requestor will, however, be notified if the initial 30 day notice period is to be extended for a further 30 days.

11. APPEAL

In contrast with the provisions in the Act relating to the establishment of an internal appeal structure in public body's, the only recourse available to a private body will be to approach a court of law.

12. CLASSES OF RECORDS HELD BY THE COMPANY

12.1. Scope

The Information contained in this chapter is intended to identify the main classes of records held within the company. Further assistance in identifying records held by the company is obtainable from the Information Officer.

12.2. Categories of records held

The following records are kept by the company :

- Financial records;
- Internal correspondence
  - Minutes of director's meetings;
  - Minutes of shareholder meetings;
  - Minutes of management meetings;
  - Correspondence with third parties – 3 years
- Agreements
  - Purchase and sale agreements;
  - Rental and lease agreements; and
  - Service and agency agreements;
- Personnel records
  - Letters of appointment;
  - Personnel information;
  - Leave records;
  - Promotion/increment increase letters;
  - Details of disciplinary hearings/matters;
  - Policies and procedures
- Information technology records and databases
- Financial records stored on server
- Software licence agreements;
- Safety records.

12.3. Further information and assistance

Further information regarding the subjects and categories or records listed herein are available from the information officer. Other information as may be prescribed by section 51(1) (f) may be obtained by the Minister of Justice and Constitutional Development.

13. PROCESSING OF PERSONAL INFORMATION

13.1. Purpose of Processing Personal information

The core reason for processing personal information in a telecommunications company is to deliver reliable communication services, manage customer relationships, ensure security, and comply with legal requirements, while respecting the privacy rights of individuals.

13.2. Description of categories of Data Subjects and of Information or categories of information relating thereto:

13.2.1. Customers (Subscribers / End-Users)

- Identification information (full name, ID number, passport number)
- Contact details (phone number, email address, physical address)
- Biometric information (where applicable for verification)
- Billing and financial information (bank details, payment history, credit records)
- Communication records (call data records, logs, data usage – where lawfully permitted)
- Location data (for service provision and network optimisation)
- Customer account information (service packages, preferences, account history)

13.2.2. Prospective Customers

- Name and surname
- Contact details (email, phone number)
- Marketing preferences
- Enquiry and quotation records

13.2.3. Employees and Job Applicants

- Identification and personal details (ID number, date of birth, gender)
- Contact information
- Employment history and qualifications
- Payroll and financial information
- Performance records and disciplinary information
- Medical information (where required and lawful)
- Background checks (criminal, credit where applicable)

13.2.4. Suppliers, Vendors, and Contractors

- Business and personal identification details
- Contact information
- Banking and payment details
- Contractual information
- Tax information (e.g., VAT numbers)

13.2.5. Business Partners and Corporate Clients

- Company representative details (names, positions)
- Contact information
- Contractual agreements and correspondence
- Financial and billing information

13.2.6. Website Users / Digital Platform Users

- IP address and device information
- Cookies and usage data
- Browsing behaviour and preferences
- Login credentials (where applicable)

13.2.7. Regulatory Authorities and Law Enforcement (where applicable)

- Information required for legal compliance and reporting
- Records related to lawful interception and disclosure obligations

13.3. The recipients or categories of recipients to whom the personal information may be supplied.

The Company may disclose personal information to the following recipients or categories of recipients, strictly in accordance with applicable laws, contractual obligations, and the principles set out in the Protection of Personal Information Act:

13.3.1. Internal Authorised Personnel

- Employees, management, and authorised representatives
- Access is limited to individuals who require the information to perform their duties

13.3.2. Service Providers and Operators

- IT service providers (hosting, cloud storage, system support)
- Network infrastructure and telecommunications service partners
- Customer relationship management (CRM) system providers
- Data analytics and processing service providers

All service providers are contractually bound to maintain confidentiality and implement appropriate security safeguards.

13.3.3. Payment Processors and Financial Institutions

- Banks and payment gateways for processing transactions
- Credit bureaus for credit vetting (where applicable)
- Debt collection agencies for recovery of outstanding amounts

13.3.4. Regulatory Authorities and Government Bodies

- Information Regulator (South Africa)
- Law enforcement agencies (e.g., SAPS)
- Communications regulatory bodies (e.g., ICASA)

Disclosure occurs where required by law or in terms of a lawful request.

13.3.5. Legal & Professional Advisors

- Attorneys, auditors, consultants, and compliance specialists
- Disclosure is limited to what is necessary for legal advice, dispute resolution, or audits

13.3.6. Business Partners and Third-Party Contractors

- Installation and maintenance contractors
- Marketing partners (only where consent has been obtained, where required)
- Outsourced customer support centres

13.3.7. Insurers

- For purposes of risk management, claims processing and asset protection

13.3.8. Other Third Parties (With consent or legal justification)

- Any other party where:
    - The data subject has provided consent; or
    - Disclosure is necessary to perform a contract; or
    - Disclosure is required or authorised by law

13.3.9. Cross-Border Recipients

- International service providers or affiliates, subject to:
  - Adequate data protection laws in the recipient country; or
  - Binding agreements ensuring POPIA-equivalent protection

Personal information is only shared with authorised recipients on a need-to-know basis, with appropriate safeguards in place to ensure confidentiality, integrity, and security, and always in compliance with applicable data protection legislation.

13.4. General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information.

The Responsible Party implements appropriate, reasonable technical and organisational measures to safeguard personal information, in line with the Protection of Personal Information Act, to ensure the confidentiality, integrity, and availability of information.

These measures include the following:

13.4.1. Governance and Risk Management

- Implementation of a formal Information Security Policy Framework
- Appointment of an Information Officer and, where applicable, Deputy Information Officers
- Regular risk assessments and privacy impact assessments (PIAs)
- Ongoing compliance monitoring and internal audits

13.4.2. Access Control Measures

- Role-based access control (RBAC) to restrict access on a need-to-know basis
- Strong authentication mechanisms (e.g., multi-factor authentication)
- User account management, including provisioning and de-provisioning processes
- Regular review of user access rights

13.4.3. Data Protection and Encryption

- Encryption of personal information in transit and at rest where appropriate
- Secure key management practices
- Masking or anonymisation of data where full identification is not required

13.4.4. Network and System Security

- Firewalls, intrusion detection and prevention systems (IDS/IPS)
- Anti-virus and anti-malware solutions
- Regular patch management and system updates
- Secure configuration of servers, databases, and endpoints

13.4.5. Physical Security Controls

- Controlled access to offices, data centres, and network infrastructure
- Use of access cards, biometric systems, and visitor logs
- CCTV monitoring of critical areas
- Secure storage of physical records

13.4.6. Incident Management and Breach Response

- Documented incident response plan
- Procedures for identifying, reporting, and managing data breaches
- Notification to the Information Regulator and affected data subjects where required

13.4.7. Data Retention and Disposal

- Defined data retention schedules in line with legal and business requirements
- Secure destruction of records (e.g., shredding, secure digital wiping)
- Regular review of stored data to ensure it is not retained longer than necessary

13.4.8. Third-Party Security Management

- Due diligence conducted on all third-party operators and service providers
- Binding agreements to ensure confidentiality and POPIA compliance
- Ongoing monitoring of third-party security practices

13.4.9. Employee Awareness & Training

- Regular POPIA and information security training for employees
- Awareness programmes on phishing, data handling, and cybersecurity risks
- Confidentiality agreements signed by employees and contractors

13.4.10. Business continuity & availability

- Implementation of backup and disaster recovery plans
- Regular data backups and testing of recovery procedures
- Measures to ensure system uptime and resilience

The Responsible Party continuously reviews and updates its security controls to address evolving threats and ensure that personal information remains protected against loss, unauthorised access, misuse, or disclosure, in accordance with applicable data protection legislation.

14. UPDATING OF MANUAL

The Information Officer of the Company, in consultation with management will on a regular basis update this manual, if and when required.

ISSUED BY

SHIRELL MAREE
HR AND COMPLIANCE ADMINISTRATOR