



Access to Information Manual in accordance with Section 51 of
the Promotion of Access to Information Act No. 2 of 2000 as
amended (PAIA)

1 Introduction

1.1 Purpose of the PAIA Manual

Section 51 of the PAIA requires a Private Body to compile an Access to Information Manual ("Manual") which sets out the procedure and requirements to be adhered to in seeking to obtain access to information held by that Private Body. The objective of the Act, as amended by section 110 of the Protection of Personal Information Act No 4 of 2013 (POPIA), is to give effect to the constitutional right of access to information outlined in section 32 of the Constitution of the Republic of South Africa.

The purpose of this Manual is to outline:

- a non-exhaustive list of the type and categories of records held by IoT.nxt (Pty) Ltd ("IoT.nxt");
- the process to submit requests for access to information;
- the grounds for refusal of access to information;
- descriptions of records which are available in accordance with any other legislation;
- relevant contact details of the Information Officer and Deputy Information Officer;
- description of the Guide on how to use PAIA, as updated by the Regulator and how to obtain access to it; and
- the Processing of Personal Information in terms of POPIA.

1.2 Contact Details for Access to Information

1.2.1 Information Officer Details

Company Registration:	2015/305236/07
Chief Executive Officer/Information Officer	Lazaros Karapanagiotidis (CEO) Renico Koen (Information Officer)
Street Address	Irene Link, Building C, Third Floor, 5 Impala Avenue, Doringkloof, Centurion 0157
Postal Address	Irene Link, Building C, Third Floor,

	5 Impala Avenue, Doringkloof, Centurion 0157
Telephone	012 880 0114
Website	www.iotnxt.com
E-mail	dpo@iotnxt.com

1.2.2 Contact Details for Access to Information

In order to ensure that IoT.nxt complies with PAIA and POPIA, the following entry points have been designated for access to information requests:

a) Are you requesting a record or description of your Personal Information held by IoT.nxt?

All Data Subjects are allowed access to their own Personal Information records or descriptions. Before submitting an access request relating to your own Personal Information, we urge any Data Subject who is a current customer of IoT.nxt to consider whether other mechanisms for receiving their information are available. The information a customer has access to includes, but is not limited to:

- Products/service information;
- Personal details related to product/service registration;
- Account details;

Please note that, where applicable, there may be reproduction costs associated with the retrieval of information records. You will be informed if such costs apply to your request.

b) Are you requesting information belonging to another person or any other records that are not classified as your own Personal Information?

In order to request other records that are not classified as your own Personal Information, please the Information Officer at dpo@iotnxt.com and follow the Request Procedure outlined in paragraph 6 below.

1.3 Availability of the Manual

A copy of the Manual is available:

- On our website at www.iotnxt.com
- the head office of IoT.nxt at the address outlined in paragraph 1.2 above for public inspection during normal business hours at no charge; and
- to any person upon request and upon the payment of a reasonable fee.

A fee for a copy of the Manual shall be payable per each A4-size photocopy made in line with the prescribed fee outlined in paragraph 7.

IoT.nxt will update this Manual on a regular basis, and the updated Manual will be published on the website.

2 Description of the PAIA Guide developed by the Information Regulator

The Information Regulator ("Regulator") has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised PAIA Guide ("Guide"), which provides information and guidance that is needed by any person who wishes to exercise any right contemplated in the PAIA and POPIA.

The Guide has been published in 10 official languages on the Regulator's website at <https://inforegulator.org.za/training/wp/paia-guidelines/>

Any questions or queries relating to the Guide published by the Information Regulator must be addressed to:

Physical Address	Woodmead North Office Park, 54 Maxwell Drive Woodmead, Johannesburg, 2191.
Phone	010 023 5200
Website	https://inforegulator.org.za
E mail	enquiries@inforegulator.org.za

3 Definitions

The following words shall bear the same meaning as under POPIA:

3.1 "**Data Subject**" means the person to whom Personal Information relates.

3.2 "**Information Officer**" means the Head of IoT.nxt, equivalent officer, duly authorised person or any person who is acting as such as contemplated in section 1 of the Act.

3.3 "**IoT.nxt**" means a private company registered in accordance with the laws of the Republic of South Africa with registration number 2015/305236/07.

3.4 "**Minister**" means the Minister of Justice and Correctional Services.

3.5 "**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including:

- a) information relating to 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;
- b) information relating to the education or the medical, financial, criminal or employment history of the person;
- c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
- d) the blood type or any other biometric information of the person;
- e) the personal opinions, views or preferences of the person;
- 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;
- g) the views or opinions of another individual about the person;
- 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.

3.6 "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information, including:

- a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- b) dissemination by means of transmission, distribution or making available in any other form; or
- c) merging, linking, blocking, degradation, erasure or destruction of information.

3.7 "**Private body**" means a natural person who carries or has carried on any trade, business or profession in that capacity, a partnership or juristic person.

3.8 "**Responsible party**" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for Processing Personal Information.

3.9 "**Requester**" in relation to a private body means any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body or any person acting on behalf of that person.

3.10 "**Vodacom Group**" means Vodacom Group Limited, registration number 1993/005461/06, a public company duly incorporated in accordance with the laws of the Republic of South Africa.

4 Categories of Records held by IoT.nxt

The categories of information listed are not exhaustive but are merely meant to give a broad indication of the information subject and categories held by IoT.nxt, without specification. A category may therefore contain sub-categories and sub-sets of information which are not specifically listed.

Record Type / Category	Description
Companies Act Records	• Broad-Based Black Economic Empowerment Verification Certificate • Codes of Conduct • Documents of Incorporation • Legal Compliance Records • Memorandum of Incorporation • Minutes of Board of Directors Meetings • Policies • Records relating to the appointment of directors/ auditors/ secretary/ public office and other officers • Shareholder register
Financial Records	• Accounting Records • Annual Financial Statements • Asset Register • Auditors' Report • Bank Statements • Banking Records • Detail of Auditors • Electronic Banking Records • Invoices • Paid Cheques • Tax Returns
Income Tax Records	• Documents issued to employees for income tax purposes • PAYE Records • Records of payments made to SARS on behalf of employees • Value Added Tax Clearance Certificate

	• All other statutory compliances: • Value Added Tax • Skills Development Levies • Unemployment Insurance Fund • Personnel Documents and Records • Attendance Registers • Disciplinary Code • Disciplinary Records • Employment Contracts • Employment Equity Plan • Leave Records • Records containing all employees' names and occupation • Salary Records • Sector Education and Training Authority Records • Training Manuals • Training Records
Income Tax Records <i>*in terms of the Consumer Protection Act No. 68 of 2008</i>	• Receipts • Correspondence • Service Agreements • Personal information such as name, contact details, company information, • work experience, educational history, race, gender • Correspondences • Customer documentation • Company and contact details of relevant individuals • Events
Supplier Records	• The name of the supplier • The address of the supplier • A description of the goods • The quantity or volume of the goods • Proof of date of payment
Supplier Records	Record of the personal information and the specific purpose for which the personal information was collected
Insurance Records	• IoT.nxt proof of General Insurance • Proof of Professional Indemnity Insurance • Directors and Officers Insurance • Cyber Insurance • Business Interruption Insurance
Immovable and Movable Property Records	• Agreements for the lease of movable property

	• Agreements for the lease or sale of land and/or other immovable property • Other agreements for the purchase, ordinary sale, conditional sale, or hire • of assets
Miscellaneous Records	Agreements for the trading activities of the business.

5 Processing of Personal Information

Note: Please access the IoT.nxt Privacy Statement [here](#).

5.1 Purpose of Processing Personal Information of Data Subjects by IoT.nxt

IoT.nxt will process Personal Information of Data Subjects based on:

- The performance of a contract with the Data Subject or entering into the contract and taking action on their requests.
- IoT.nxt's legitimate business interests include fraud prevention, tax evasion, and financial crime prevention, as well as maintaining the security of its network and services and improving services.
- Protecting Data Subject's legitimate interests - for example, providing notifications regarding network availability and performance in their area, notification of emergency services, and fraud prevention.
- Compliance with a mandatory legal obligation, including accounting and tax requirements, which are subject to strict internal policies and procedures, and Data Subject's right to restrict usage of their Personal Information, which controls the scope of legal assistance to be provided. IoT.nxt is also required to process Personal Information pursuant to legislation including but not limited to the Financial Intelligence Centre Act, 38 of 2001 (FICA), the Regulation of Interception of Communications and Provisions of Communication-related Information Act 70 of 2002 (RICA), the Electronic Communications and Transactions Act, 2002 (ECTA), the Electronic Communications Act, 2005 (ECA), the Consumer Protection Act, 2008 (CPA), the Promotion of Access to Information Act, 2000 (PAIA), and the Cybercrimes Act, 2020.
- Data Subject consent where IoT.nxt does not rely on another legal basis (referred to above). Consent may be withdrawn at any time. When Data Subjects give their consent, they will be given details on how to change their mind.

The purpose for which Personal Information is processed by IoT.nxt will depend on the nature of the services or products being provided to the Data Subjects. Below are some purposes for Processing Personal Information:

- to provide Data Subjects with products and services;
- to bill Data Subjects for using IoT.nxt's products and services or to take the appropriate amount of credit;
- contact Data Subjects if the billing information they provided is about to expire or IoT.nxt is not able to take payment;
- to respond to any questions or concerns about its network, products or services;
- to provide roaming services;
- for employment purposes;
- managing third-party relationships;
- managing its networks and understanding network usage;
- marketing and tailoring services to Data Subjects;
- to contact Data Subjects with customer service messages to keep them updated with current information about products and services they have taken. For example, changes to our terms and conditions or service interruptions;
- to deliver advertising to Data Subjects;
- credit checks, fraud prevention and security;
- to manage visits by different stakeholders to any IoT.nxt premises;
- for research and analytics.

5.2 Categories of Data Subjects and their Personal Information

IoT.nxt holds information and records relating to the following Data Subjects. Please note that this list is non-exhaustive:

- a) employees /personnel of IoT.nxt;
- b) clients/customers of IoT.nxt;
- c) any third party and/or supplier with whom IoT.nxt conducts its business;
- d) contractors of IoT.nxt;
- e) partners and agents;
- f) service providers of IoT.nxt;
- (g) Requesters in terms of PAIA and POPIA.

The categories of Personal Information that IoT.nxt processes of the Data Subjects defined below include the following:

- Full names, addresses, phone and/or mobile numbers, date of birth, gender, information about their property or household, and e-mail address.
- Credit or debit card information - information about bank accounts and other banking information. For example, when a Data Subject opens an account with IoT.nxt or processes a payment whenever they make a purchase.
- Location data - this can be precise where it uses Global Positioning System (GPS) data or by identifying nearby mobile phone and Wi-Fi hotspots, and the Data Subject enables location-based services or features. It can also be less precise where, for example, a location is derived from the Data Subject's IP address or data such as a postcode or name of a town or city.
- Correspondence - such as a note or recording of an e-mail or letter sent or other records of any contact with IoT.nxt.
- Account information - such as dates of payment owed or received, subscriptions, account numbers or other information related to an account.
- Credential information – IoT.nxt collects passwords, hints and similar security information used for authentication and access to accounts and services.
- Preferences for particular products and services.
- Data sessions - to enable connection to be made and for billing purposes, fraud investigations, network and store planning, campaign planning, marketing specific products such as URL bundles, identifying visits to competitor websites, and personalisation of services.
- Photographs and images - when attending any of IoT.nxt's events or functions or accessing premises with surveillance cameras.
- Information obtained from other sources, such as credit agencies, fraud-prevention agencies, and other data providers. This includes demographic data and interest-based data.

5.3 The recipients or categories of recipients to whom the Personal Information may be supplied by IoT.nxt

IoT.nxt may supply information or records of information to the following categories of recipients:

- a) its employees as part of executing its business functions;
- b) statutory oversight bodies, regulators (such as the Information Regulator), law enforcement agencies or judicial commissions of enquiry making a request for information;

- c) any court, administrative or judicial forum, arbitration, statutory commission, or ombudsman making a request for data or discovery in terms of the applicable rules;
- d) South African Revenue Services, or another similar authority;
- e) emergency Service Organisation (if the Data Subject make an emergency call), including their approximate location;
- f) anyone making a successful application for access in terms of PAIA, to the extent that such access is permitted in terms of PAIA, as amended by POPIA.;
- g) subject to the provisions of POPIA and the National Credit Act No. 34 of 2005, IoT.nxt may share information about a client's creditworthiness with any credit bureau or credit providers;
- h) debt collection agencies or other debt-recovery organisations;
- i) any third party and/or supplier with whom IoT.nxt conducts its business;
- j) contractors of IoT.nxt;
- k) partners and agents;
- l) service providers of IoT.nxt;
- m) third parties that we use to provide you with marketing and advertisements;
- n) companies in the Vodacom and Vodafone Group; and
- o) verification agencies for employment purposes.

5.4 Planned trans-border flows of Personal Information

IoT.nxt does transfer Personal Information of Data Subjects across borders, including but not limited to countries in the European Union, United States of America, United Kingdom, Australia and to the Vodafone and Vodacom group companies and/or authorised third parties beyond the borders of the countries to achieve a defined purpose. The defined purposes include the:

- 1) achievement of its business functions;
- 2) provision of products and services that the customer has requested;
- 3) hosting or storage of some of its systems and infrastructure;
- 4) data warehousing activities;
- 5) the provision of centralised business activities within the Vodafone and Vodacom group of companies, such as where we share technology and resources.

IoT.nxt will only engage in the cross-border transfer of information if one of the following conditions are met and the transfer has been assessed and approved by the Information Officer:

- The recipient is subject to existing legislation in his /her/it's country, a binding corporate or binding agreement that provides an adequate level of

protection for the personal information that is substantially similar to the data protection laws applicable to South Africa;

- The Data Subject has consented to such cross-border transfer;
- The transfer is necessary for the conclusion and/or performance of a contract between IoT.nxt and the Data Subject;
- The transfer is necessary for the conclusion or performance of a contract entered into, in the interest of the Data Subject, between IoT.nxt and the relevant Vodacom Group company or the Authorised Third Party;
- The transfer is to the benefit of the Data Subject and must take place in circumstances under which it is not reasonably possible to obtain the Data Subject's consent, and if it were reasonably possible to obtain such consent, the Data Subject would be likely to give it.

The processing of Personal Information in a foreign jurisdiction may be subject to the laws of the country in which it is held and may be subject to disclosure to the Governments, Courts of law, Enforcement or Regulatory Agencies of such other country, pursuant to the laws of such country. As a measure, IoT.nxt conducts Transfer Impact Assessments to assess the legislative framework that governs disclosures of information in jurisdictions where information is transferred and implements security and contractual measures to limit the risk exposure. However, where such disclosures are required, IoT.nxt will ensure the adequate protection of your Personal Information.

5.5 General Description of Information Security Measures

- IoT.nxt is committed to continuously implementing security safeguards to protect Personal Information. For this reason, IoT.nxt has specialised security teams that constantly review and improve its measures to secure the integrity and confidentiality of Personal Information by taking appropriate, reasonable technical and organisational measures to protect it from unauthorised or unlawful access, accidental loss, damage, disclosure or destruction.
- If IoT.nxt has an agreement with another organisation to provide services on its behalf, IoT.nxt will take reasonable steps to ensure that they have appropriate security measures in place that are substantially similar to the security measures implemented by IoT.nxt. These organisations will not be entitled to use Personal Information for their own purposes. If necessary, the security teams will conduct an audit on them to ensure they meet IoT.nxt's security requirements.
- IoT.nxt has implemented various information security measures such as, but not limited to:

- o Firewall and network endpoint protection;
- o Antivirus and Multifactor Authentication;
- o A dedicated support network of cyber security professionals;
- o Encryption and/or similar cryptographic technologies and techniques;
- o Access control methodologies based on user roles and security clearance levels;
- o Confidentiality protocols that apply to all internal documents and correspondence; and/or
- o Disaster Recovery and Business Continuity Management Protocols and Procedures.

6 Request Procedure

6.1 Procedure to be followed by the Requester

- A request for access to a record must be made in a prescribed Form 2 (Annexure A) to IoT.nxt at its address or electronic e-mail address outlined in paragraph 1.2.2.
- The Requester must provide sufficient information for identification purposes. Therefore, proof of identity is required to authenticate the Requester, such as a certified copy of their identity document, driver's license or passport.
- If the request is made on behalf of another person, the Requester must provide proof of the capacity in which they are making the request and authorisation to make such request.

A request which does not comply with the formalities contained in this Manual (including Forms not completed correctly) will be referred back to the Requester with advice on the necessary steps for compliance.

Note: Information will not be furnished unless a person clearly provides sufficient particulars to enable IoT.nxt to identify the right the Requester seeks to protect as well as an explanation of why the requested information is required for the exercise or to protect that right.

6.2 Procedure to be followed by IoT.nxt after receipt

The following procedure will be followed by IoT.nxt after receipt of the request for access:

- Once a request is made in the prescribed Form 2, IoT.nxt will send an acknowledgement of receipt.
- The Requester will receive notice from IoT.nxt to pay a request fee of R140.00 (if applicable).
- The prescribed fee must be paid before the request is processed.
- Payment of this fee should be made as directed by IoT.nxt.
- If the request is granted, then the Requester might be required to pay a further access fee for the search, reproduction and preparation of the record and for the time that has exceeded the prescribed hours to search and prepare the record for disclosure.

6.3 Guidance for completing the Request Form

The Requester can contact IoT.nxt using the details outlined in paragraph 1.2.2 for guidance on how to complete Form 2, as well as the documents that need to be submitted or applicable fees.

An oral request for access to a record(s) may be made as a result of the Requester's illiteracy or disability. The Information Officer /Deputy Information Officer will assist the Requester in completing the prescribed form on behalf of such Requester and provide him/her with a copy of the completed form.

6.4 Response Time

- All requests complying with the requirements set out above will be processed, and a written notice of the decision will be provided to the Requester within 30 days of receiving the completed Form 2. In case of a request being refused, the notification will include the reasons for the refusal.
- IoT.nxt may request an extension of the 30-day notice period for a further period not exceeding 30 days due to the nature of the request and the amount of time required to gather the requested information.
- IoT.nxt will make the extension request prior to the expiry of the 30-day period and provide reasons for the extension.

6.5 Granting or Refusal of a Request

6.5.1 If the request for access is granted, then IoT.nxt will advise the Requester of:

- the prescribed reproduction fees for accessing the information or documentation,
- payable deposit fee and balance outstanding (if any),
- the form in which access will be given, and

- the right to lodge an application in court or complain to the Information Regulator against the access fee to be paid or the form of access to be granted within 180 days of IoT.nxt notifying the Requester of its decision.

6.5.2 If the request for access is refused, IoT.nxt will advise the Requester about the reasons for the refusal of access and may advise the Requester that they may lodge an application in court or complain to the Information Regulator against the refusal of the request.

6.5.3 Chapter 4 of the PAIA stipulates the following grounds for refusing requests for information:

- protection of the privacy of a third party who is a natural person;
- protection of commercial information of a third party;
- protection of certain confidential information of a third party;
- protection of the safety of individuals and protection of property;
- protection of records privileged from production in legal proceedings;
- commercial information of the Private Body;
- protection of research information of a third party and of the Private Body.

6.5.4 These grounds of refusal are also endorsed in section 23(4)(a) of POPIA. If a request for access to Personal Information is made and part of that information may or must be refused in terms of PAIA, every other part will be disclosed.

6.6 Records that cannot be located or do not exist

Where records cannot be located but to which a Requester would have had access if the record was available, IoT.nxt will provide a response in the form of an affidavit or affirmation. This also applies where the requested records do not exist.

7 Prescribed Fees

The Act entitles a Private Body to levy a prescribed fee to a Requester before further Processing the request.

According to section 23(3) of POPIA, a Responsible Party may require payment of a prescribed fee for the provision of a record of Personal Information about the Data Subject in its possession. IoT.nxt will provide the Requester with a written estimate of the fee before providing the services and may require the Requester to pay a deposit for all or part of the fee.

Please see below the prescribed fees applicable that have been published in the Annexure B of PAIA Regulations, 2021.

Item	Description	Amount
1	Request fee payable by every Requester	R140.00
2	Photocopy/printed black and white copy of a A4-size page	R2.00 per page or part thereof
3	Printed copy of A4-size page	R2.00 per page or part thereof
4	For a copy in a computer-readable form on a flash drive (provided by the Requester)	R40.00
5	For a copy in a computer-readable form on compact disc (if provided by Requester)	R40.00
6	For a copy in a computer-readable form on compact disc (if provided to the Requester)	R60.00
7	For a transcription of visual images per A4-size page	Services to be outsourced, will depend on quotation from Service Provider
8	Copy of visual images	
9	Transcription of an audio record per A4-size page	R24.00
10	For a copy of an audio record on a Flash drive (to be provided by Requester)	R40.00
11	For a copy of an audio record on a compact disc (if provided by Requester)	R40.00
12	For a copy of an audio record on compact disc (if provided to the Requester)	R60.00
13	To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation To not exceed a total cost of:	R 145.00 R 435.00
14	Deposit: If search exceeds 6 hours.	One third of the amount per request calculated in terms of above items
15	Postage, e-mail or any other electronic transfer	Actual expense, if any

IoT.nxt, as a private body registered under the Value Added Tax Act, 1991 will add VAT to all the above-mentioned fees.

8 Lodgement of Complaints

The Act makes provision for the lodgement of a complaint to the Information Regulator by any person who alleges that the decision was not in compliance with the Act for refusing access, aggrieved by a decision regarding fees prescribed, the extension of the period within which the request must be dealt; or refusing access in the form requested by the Requester. The complainant may also apply to a court with appropriate jurisdiction. The complaint to the Information Regulator must be in the prescribed manner and form as published on the website of the Information Regulator and lodged within 180 days of the decision from IoT.nxt.