KHIPU | CYBER SECURITY

PAIA and FOIA Manual

KHIPU Networks Limited
(and its subsidiaries associated)

VERSION: 3

DATE: 25th June 2026

By Royal Appointment to
His Majesty The King
Cyber Security Provider
KHIPU Networks Limited
Hampshire

Date of Issue:	25th June 2026
Document Version and Reference:	3
Controlling Author(s):	John Ayres
Approval:	Andrew Brimson

KHIPU Networks holds certification to the following standards, which are audited independently by external accrediting bodies:

- ISO9001 Quality Management
- ISO27001 Security Management
- ISO14001 Environmental Management
- ISO45001 Occupational Health and Safety
- Cyber Essentials Plus
- NCSC Cyber Incident Response (CIR): Standard Level
- CREST: Cyber Incident Response

KHIPU Networks supports the National Apprenticeship Scheme and employs and develops apprentices within all sectors of the company.

KHIPU Networks Limited
Company Number: 5218573
Switchboard: +44 (0)345 272 0900
Support: +44 (0)345 272 0910

UK Office
3 Waterfront Business Park
Fleet
Hampshire
GU51 3TW

sales@khipu-networks.com
@KHIPUNetworks
www.khipu-networks.com

KHIPU Networks South Africa (PTY) Limited
Company Number: 2012/180716/07
Switchboard: +27 (0)41 393 7600
Support: +27 (0)41 393 7601

Gqeberha Office
Greenacres Office Park
78-84 2nd Avenue
Newton Park
Gqeberha

Cape Town Office
13 Waterford Mews
Century City
Cape Town

TABLE OF CONTENTS

1. Introduction

Under the Freedom of Information Act (FOI) in the United Kingdom and the Promotion of Access to Information Act (PAIA) in South Africa, this manual has been produced to provide the public with the following information:

- Records held by the company which are available without having to ask for them.
- An understanding of how to make a formal request for information.
- The classification of records which can be made in line with legislation.
- To demonstrate compliance with the additional requirements of POPIA and GDPR.

This guide is available in the English language only and is accessible from all of our office locations as defined in page two of this manual, as well as on our website.

2. About KHIPU Networks

We are a privately owned award winning international Cyber Security Company delivering a wide range of network, wireless and security solutions, technologies, and services across multiple sectors. Founded in 2005, KHIPU Networks' ethos has always been to work in partnership with customers, to understand their environments and challenges so that we can design and deploy 'Best of Breed' solutions that enable them to meet their strategic goals.

KHIPU Networks expanded to Africa in 2012 and have an office in Mauritius and two offices in South Africa which includes a Security Operations Centre (SOC) to increase the reach and functionality of our managed services, specifically our Managed Security Service Provider (MSSP) focus.

KHIPU's main focusses as a business are:

- To provide 'outstanding' commercial and technical customer services.
- To work in partnership with our customers to understand their environments and challenges so that we provide 'best of breed' solutions to meet their strategic goals.
- To have exceptional customer references, enabling our business to grow and who will provide testimonials to customers who are considering our solutions.

3. Legislation

KHIPU are obliged to abide by all relevant UK and South African legislation. This requirement devolves to the employees and agents of the company who may be held personally responsible for any breaches, which includes the following from a data management perspective:

3.1. The Data Protection Act

The provisions of this act relate to all personal data of living persons and covers:

Fair and lawful obtaining of data
No person should be misled about the uses, potential or real, which may be made of the information they provide.

Purpose of Information
The Register Entry for the Company, which is held by the Data Protection Registrar in accordance with the Act, contains particulars of personal data held by KHIPU.

If any staff member is uncertain of the legality of storing or processing particular data items, they shall request clarification from a Board member.

Use or Disclosure of Information
Information stored in any system shall be used and disclosed only in accordance with the Register Entry. Any breach of this principle may lead to prosecution of an individual.

3.2. The General Data Protection Regulation (GDPR)

The requirements of this regulation form part of the Data Protection Act 2018. The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.3. Copyright, Designs and Patents Act

All computer software used on any automated information system in KHIPU must be properly licensed. KHIPU may be prosecuted if illegal software is found to be resident on any one of the information systems in use, including laptop computers and other portable devices used outside the normal boundaries of the company.

The Technical Department shall be responsible for conducting software audits at periodically to ensure that all software has been properly procured and licensed. However, it shall remain the individual responsibility of all staff or agents of KHIPU to monitor systems under their control for the existence of illegal software.

No member of staff or agent of KHIPU shall copy software illegally, nor introduce illegally copied or any other unauthorised software into any part of the information systems, nor knowingly use illegally copied software. Any person who does shall be subject, upon discovery, to disciplinary action.

3.4. The Computer Misuse Act

The purpose of this legislation is to ease the prosecution of persons who access systems when they are unauthorised to do so.

It is necessary to ensure that all members of staff understand the seriousness of accessing parts of any system to which they have not been given access rights. Notice is hereby given that KHIPU intends to pursue prosecution of those who attempt to extend their legitimate scope of access for unauthorised purposes.

3.5. The Freedom of Information Act (FOIA)

This legislation provides public access to information held by public authorities, or by companies who hold information on or on behalf of a public authority. The Act covers any recorded information that is held by a public authority in England, Wales, and Northern Ireland, and by UK-wide public authorities based in Scotland.

Public authorities include government departments, local authorities, the NHS, state schools and police forces. Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

The Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, they should make a data protection subject access request.

3.6. Protection of Personal Information (POPIA)

POPIA gives effect to the common law and constitutional right to privacy and regulates the manner in which the personal data of individuals (data subjects), including website users, can be "processed" (that is, collected, held, used, modified, disclosed, or transferred) by among other things, a data controller ("responsible party" in POPIA). POPIA imposes duties on data controllers in deciding how and why such information is processed.

3.7. Data (Use and Access) Act

The Data (Use and Access) Act 2025 introduces targeted reforms to the UK data protection framework to simplify compliance and support responsible data use. While it does not replace existing legislation such as UK GDPR, it provides greater flexibility for organisations in certain areas, including data processing, automated decision-making, and subject access requests.

Organisations must continue to meet core data protection obligations, while ensuring that updated requirements, ensuring that disclosure obligations are balanced against data protection requirements to prevent unlawful disclosure of personal data.

4. Data Classification

All data and documents received, produced, or viewed by KHIPU shall be classified under one of the following headings (in the order of importance with the highest first).

4.1. Company Classified

KHIPU’s information whose unauthorised disclosure (even within the organisation) would cause damage to the interests of the company. It would normally inflict harm by virtue of financial loss, loss of profitability, opportunity, embarrassment, or loss of reputation. This type of information would include:

- Details of major acquisitions, investments, and mergers
- High-level business and competition strategy
- High-level business plans and potential options
- Personnel Records
- Product Development Strategy
- Company Security System data

4.2. Customer Confidential

Customer information whose unauthorised disclosure would cause harm to the interests of the customer, or customer relationship. This would normally inflict harm by virtue of financial loss; loss of profitability, opportunity; embarrassment, or loss of reputation. This includes, but is not limited to, customer information covered by non-disclosure agreements.

4.3. Company Confidential

KHIPU's information whose unauthorised disclosure, particularly outside the organisation, would be inappropriate and inconvenient. This is routine information which the organisation simply wishes to keep private.

- Company financial data: Access to this data needs to be restricted for commercial reasons.
- Customer quotations and order information.
- Company Commercial Issues: Disclosure of critical business issues prematurely require consideration e.g. new acquisitions, changes in company structure or changes in staff.
- New product development.

4.4. Unclassified

This applies to any data or information in any format that can be disclosed without authorisation or used without any controls applied.

5. Personal Information Processing

5.1. Employees

KHIPU uses employees' information to manage working arrangements and the relationship between employees and the company via employment contractual agreements, fulfilment of their roles and compliance with legal obligations.

Information on the health of employees' is used to comply with health and safety regulations and to manage instances of sick leave, access to benefits, and travel requirements.

The company reserves the right to monitor any real-time, stored, or archived communication when employees are using the company's communications services/platforms.

Third parties may be used to assist with verifying some of the information employees have shared with KHIPU i.e. confirmation of the attendance of external provided courses, receiving qualifications etc.

KHIPU collects biometric information on employees for facial recognition access to our offices and its floors. CCTV cameras are also in place to monitor activity within our offices. In the event of a security incidents such as theft or fraud, the company reserves the right to share this information with the police.

5.2. External Personnel

If you work for one of our customers, suppliers or business partners, the information we collect about you may include your contact information, details of your employment and our relationship with you. This information may be collected directly from you or provided by your organisation.

Your organisation should have informed you that your information would be provided to us and directed you to our privacy policy here. We use this as necessary for our legitimate interests in managing our relationship with your organisation. If we have a business relationship with you or your organisation, we may receive information about you from your organisation.

We keep this information for up to seven years after the end of our relationship with your organisation.

6. Requesting Information

Under PAIA, a person can only request information if it is required for the protection of a legitimate right. As such, reasoning for any request should be made to allow the company to assess as required. The exercise of an individual's rights is subject to justifiable limitations, including but not limited to the reasonable protection of privacy, good governance, and commercial confidentiality. Requests cannot be made for access to a record for criminal or civil proceedings, or after commencement of proceedings as such.

Any requests must be marked 'FAO Legal Department' as per the Contact Details section of this manual. You must also enclose your proof of identity, such as a certified copy of your identity document or other legal forms of identity in order to authenticate the request.

Requests made within the instructions set out in this manual will be processed within 20 working days, unless the request contains considerations which justify extra time being required. In a situation where an extension is required, you will be advised of this and will receive an explanation to why the extension is required.

Fees payable will also be confirmed by a member of the Legal department at the time of fulfilling the request.

6.1. Particulars of Requested Record

To properly process a request further to the section above, any request made to the Legal department via email, or a letter will need to contain the following:

- Description of the record or relevant part
- Reference number, if known and available
- Reason for the request and any further information which should be considered
- The type of record i.e. printed, held on a machine, audio, or imagery
- Form of access (if the request is accepted) i.e. a printed copy of the record, a copy on a flash drive or CV etc.
- Where to send the record (if the request is accepted) i.e. a postal or email address.
- The manner of correspondence i.e. responses to requests via portal or email address.

6.2. Refusal of Requests

There are various reasons which a request could be refused, including but not limited to:

- The request not complying with PAIA legislation. Grounds for refusal of the data subject's request is set out in PAIA.
- Protection of personal information that belongs to a third person from unreasonable disclosure.
- Protecting commercial information, such as financial and commercial details, which belong to a third party.
- Disclosure resulting in the breach of a confidentially agreement that the company has with a third party.
- Information being shared that could jeopardise the safety or impair certain property rights of an individual.
- If the record was produced during legal proceedings, or if a record is being used during ongoing legal matters.

- Protecting information that is deemed company classified or confidential.
- If the record contains any information about research being carried out or about to be carried out by the company or a third party that it has employed to do so.

There are no grounds for appeal if a request is refused as a decision by a representative of the Legal department is final. You are entitled to apply to a court to take this further in a scenario where this happens.

6.3. Fees Payable

No:	Description	ZAR Amount	GBP Amount
1	Request fee, payable to every requester	R140.00	£7.00
2	Photocopy or printed copy for A4-page or A4 size-page (whether part page or full page)	R2.00 per page	10p per page
3	Digital copies or audio recordings on portable media, or compact discs provided by the requester	R40.00	£2.00
4	Digital copies or audi recordings on portable media, or compact discs provided by to the requester	R60.00	£3.00
5	For each hour or part of the hour (excluding the first hour) reasonably required to search for and/or prepare records to satisfy the requesters requirement	R145.00 per hour	£7.25 per hour
6	Deposit: if the search exceeds 6 hours	Variable	Variable
7	Postage, email, or any other electronic transfer	Variable	Variable

7. Contact Details

Any enquiries regarding the manual and requests for information can be made to the following:

Team: FAO Legal Department
Telephone: +27 (0)41 393 7600
E-mail: legal@khipu-networks.com
Postal Address: As per page 2 for our UK, Gqeberha and Cape Town offices

8. Updates

The company commits to reviewing this manual annually, where availability will be on our website, at our offices or available upon request from the Legal department.

9. Version History

Version	Date	Change
1	15/05/2024	Approved release
2	26/06/2025	General review
3	25/06/2026	Information added on the Data (Use and Access) Act under the Legislation section.