CYBERLINX

People | Process | Technology

Cyberlinx PAIA Manual

CX-GOV-MAN-001

Prepared in terms of section 14 of the Promotion of Access to Information Act 2 of 2000 (as amended)

Date Of Compilation:19/04/2022
Date of Revision: 31/07/2024

Table of Contents

1 DOCUMENT REVISION HISTORY

Date	Edited by	Designation	Version	Comment
19/04/2022	Andrew Sjoberg	Chief Technology Officer	1.0	Compiled
31/07/2024	Andrew Sjoberg	Chief Technology Officer	1.0	Reviewed and Approved for Use

2 DOCUMENT APPROVAL

Designation	Name	Date	Signature
Approved by	Andrew Sjoberg	31/07/2024	

3 LIST OF ACRONYMS AND ABBREVIATIONS

3.1 Internal Abbreviations

3.1.1 "MD" Managing Director
3.1.2 "DIO" Deputy Information Officer;
3.1.3 "IO" Information Officer;
3.1.4 "Minister" Minister of Justice and Correctional Services;
3.1.5 "PAIA" Promotion of Access to Information Act No. 2 of 2000(as
3.1.6 Amended;
3.1.7 "PFMA" Public Finance Management Act No.1 of 1999 as
3.1.8 Amended;
3.1.9 "POPIA" Protection of Personal Information Act No.4 of 2013;
3.1.10 "Regulator" Information Regulator.

4 PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to:

- Check the nature of the records which may already be available at Cyberlinx Security, without the need for submitting a formal PAIA request;
- Have an understanding of how to make a request for access to a record of Cyberlinx Security;
- Access all the relevant contact details of the persons who will assist the public with the records they intend to access;
- Know all the remedies available from Cyberlinx Security regarding request for access to the records, before approaching the Regulator or the Courts;
- The description of the services available to members of the public from the Cyberlinx Security, and how to gain access to those services;
- A description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;
- If the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;
- Know if Cyberlinx Security has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and
- Know whether Cyberlinx Security has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

5 ESTABLISHMENT OF CYBERLINX SECURITY

The Management Committee of Cyberlinx has determined the boundaries and applicability of the information security management system to establish its scope for certification and includes:

- Internal and external issues.
- Interfaces and dependencies between what is happening within the ISMS

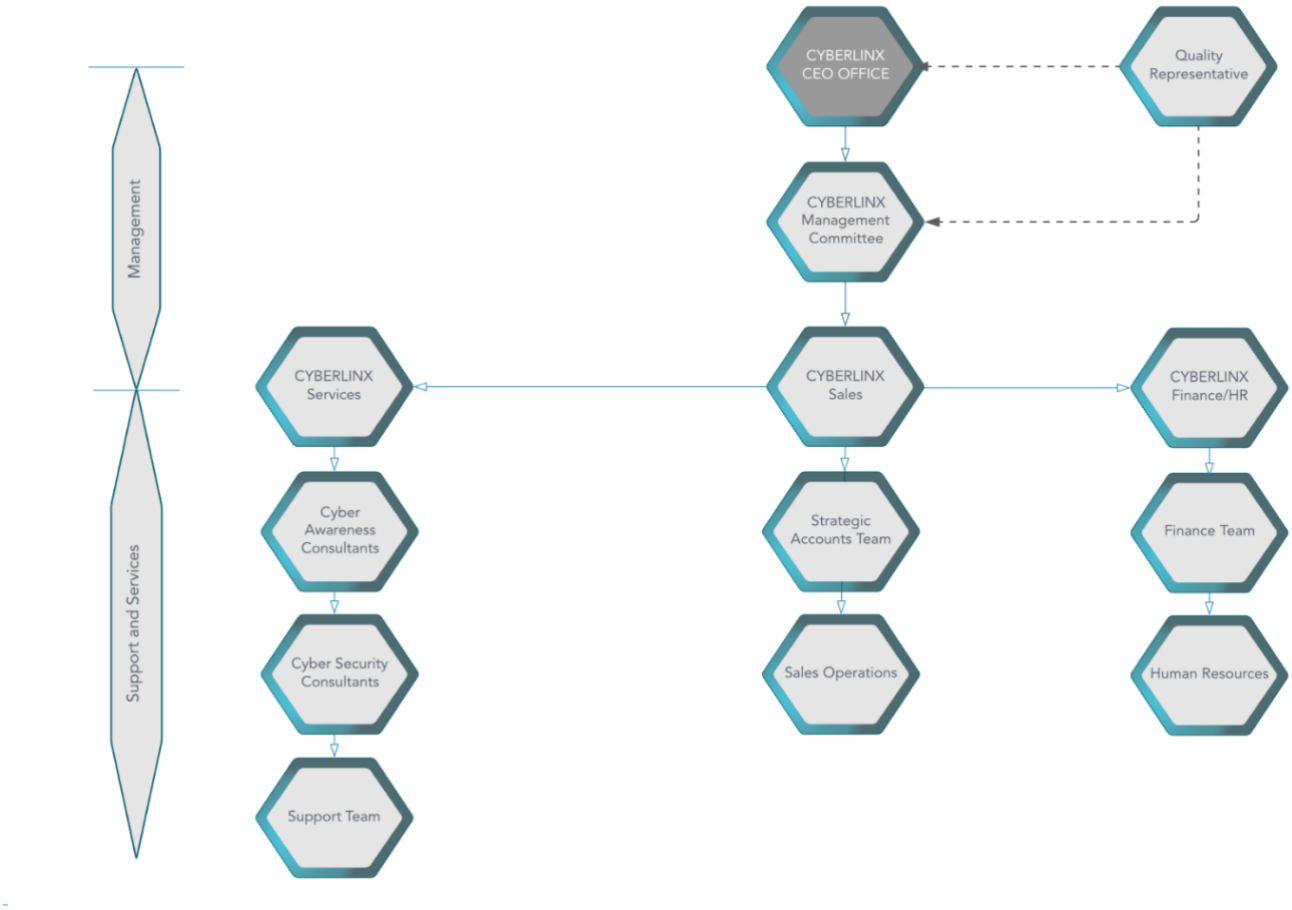
Our information management security system satisfies the requirements of ISO 27001:2013 and, based on our understanding of our business and the needs and expectations of our stakeholders, addresses and supports our processes at our head office in Bryanston as well as work performed remotely by our staff, for management, administration and the design, development, and provision of our products and services.

Cyberlinx 's scope of services includes products related to services below:
- Cyber Awareness Training
- Penetration Testing
- Cloud Security Consulting
- Cyber Security Consulting
- Managed services

6 STRUCTURE OF CYBERLINX SECURITY

6.1 Structure

Cyberlinx has established an organizational structure to implement and maintain the Information Security Management System. The high-level organisational structure is as follows:



Responsibilities and authorities are communicated through organizational charts and documented job specifications. All managers are expected to demonstrate their commitment to the development and improvement of our information security management system through:

- the provision of necessary resources;
- their involvement in the internal audit process;
- their proactive involvement in continual improvement activities; and
- focusing on the improvement of key system processes

The following responsibilities and authorities have been defined, specifically for the implementation and maintenance of the Cyberlinx Information Security Management System:

Role	Responsibilities
Cyberlinx Management Committee	Defining the context of the security program including aligning the program to business objectives and ensuring appropriate stakeholders have been considered Setting the strategic objective, building the security program road-map, allocating budget and human resources Developing, tracking, and reporting security objectives and targets to relevant stakeholders Attending scheduled management review meetings and communication of results to the organisation

Role	Responsibilities

Internal audit team	Drafting the annual internal audit plan Executing against the audit plan Reporting results to the Management Committee Follow up on corrective action implementation
ISMS Management Representative	Control of Documented Information
Human Resources Business Partner	Resource Management
Control Owners	Security operations such as vulnerability management, intrusion monitoring, and active defence, network engineering and permitter support, availability of systems, including back-up and restoration.
Risk Management Committee	Attendance to Risk Management meetings Defining the risk management process including risk analysis, risk measurement, and risk treatment Overseeing the annual risk assessment including periodically reviewing the risk register Reviewing, approving, socializing, and enforcing policy decisions across the organization Reviewing results of security assessments and other security related activities Assisting with Incident Management and Incident Response
Managers	Basic end-user security awareness training Training based on regulatory or contractual requirements Implementation of the policies, processes and systems described in this manual and for planning, controlling and resourcing our information security management system processes within their area of responsibility.
All employees	Implementation of, and adherence to the policies and procedures applicable to processes they perform. All employees are encouraged to identify and report any known or potential problems and to recommend related solutions.

7 KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF CYBERLINX SECURITY

7.1 Chief Information Officer

Name: Andrew Sjoberg
Tel: 079 030 9139
Email: andrew@cyberlinx.co.za

7.2 Deputy Chief Information Officer

Name: Russell Wells
Tel: 078 5656 159
Email: russell@cyberlinx.co.za

7.3 Access to Information General Contact

Email: info@cyberlinx.co.za
Email: Brenda@cyberlinx.co.za

7.4 National Head Office

Postal address: 2nd Floor, Building 1, Silverpoint Office Park, 22 Ealing Crescent, Bryanston, 2191
Physical Address: 2nd Floor, Building 1, Silverpoint Office Park, 22 Ealing Crescent, Bryanston, 2191
Telephone: 010 009 5334
Email: Info@cyberlinx.co.za
Website: www.cyberlinx.co.za

8 DESCRIPTION OF ALL REMEDIES AVAILABLE IN RESPECT OF AN ACT OR A FAILURE TO ACT BY CYBERLINX SECURITY

8.1 General

The Cyberlinx Management Committee has developed our Information Security Objectives, which are to:
- ensure that we can continue operations with minimal disruptions
- ensure absolute integrity for all information that we disperse or produce
- manage all information with appropriate confidentiality
- minimise information security incidents

These objectives take into account our information security requirements and those risks and opportunities that we have identified.

The Cyberlinx Management Committee ensures that our Information Security Objectives are:
- consistent with our Information Security Policy
- measurable (if practicable)
- monitored
- communicated
- updated as appropriate

Progress towards achieving each target, and the targets themselves, are reviewed during Management Review Meetings and updated as necessary.

The Security Objectives and Targets are documented in CX-GOV-PLN-004 Information Security Management System Objectives and Targets.

8.1.1 Planning actions to achieve our Information Security Objectives

Cyberlinx has established information security objectives at relevant functions, levels, and processes needed for the effective operation of our Information Security Management System. These objectives are:
- consistent with the Information Security Management Policy;
- measurable;
- based on applicable requirements;
- relevant to conformity of products and services and to enhancement of customer satisfaction;
- monitored;
- communicated; and
- updated as appropriate.

9 GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

- The Regulator has, in terms of section 10(1) of PAIA, updated and made available the revised Guide on how to use PAIA (“Guide”), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.
- The Guide is available in each of the official languages
- The aforesaid Guide contains the description of:
    - The objects of PAIA and POPIA.
    - the postal and street address, phone and fax number and, if available, electronic mail address of
        - The Information Officer of every public and private body, and
        - Every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA1 an section 56 of POPIA2
    - The manner and form of a request for
        - access to a record of a private body contemplated in section 504;

- the assistance available from the Information Officer of a public body in terms of PAIA and POPIA;
- the assistance available from the Regulator in terms of PAIA and POPIA;
- all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging.
  - An Internal Appeal
  - A complaint to the regulator
  - An application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body.
- The provisions of sections 145 and 516 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
- The provisions of sections 157 and 528 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;
- The notices issued in terms of sections 229 and 5410 regarding fees to be paid in relation to requests for access; and

- Members of the public can inspect or make copies of the Guide from the offices of the public or private bodies, including the office of the Regulator, during normal working hours. The Guide can also be obtained
  - upon request to the Information Officer;
  - from the website of the Regulator (https://www.justice.gov.za/inforeg/).

10 CATEGORIES OF RECORDS OF CYBERLINX SECURITY WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

The table below describes categories of Cyberlinx Security records which are available without a person having to request access in terms of this Act. The table also lists the type of document and how the document can be accessed. These are not necessarily records that may be available on the website, however a person may request a document telephonically or by sending an email or a letter.

Category of Record	Document Type	Available On Website	Available On Request
Human Resources:	HR Policies and Procedures Employee Records Advertised Posts	No No Yes – Linked'In	Yes Yes Yes
Legislation /Regulations/Certifications	Memorandum of Incorporation PAIA Manual (Promotion of Access to Information Act 2 of 2000)	No No https://www.cyberlinx.co.za	Yes Yes
Strategic Documents	N/A	N/A	N/A

11 SERVICES AVAILABLE TO MEMBERS OF THE PUBLIC FROM CYBERLINX SECURITY AND HOW TO GAIN ACCESS TO THOSE SERVICES.

Cyberlinx Security offers a wide range of services to members of the public aimed at enhancing digital security and safeguarding against cyber threats. These services include:

Cyber Security Consultations: Tailored advisory sessions to assess and address individual or organizational security needs.

Vulnerability Assessments: Comprehensive evaluations to identify and mitigate potential weaknesses in digital infrastructure.
Penetration Testing: Ethical hacking simulations to uncover vulnerabilities and fortify defenses.
Security Awareness Training: Educational programs to empower individuals and teams with best practices for cyber hygiene.

To gain access to these services from Cyberlinx Security, individuals and organizations can follow these steps:

Initial Consultation: Contact Cyberlinx Security to schedule an initial consultation to discuss specific security requirements and objectives.
Service Selection: Based on the consultation, choose the appropriate services that align with your needs, whether it's a vulnerability assessment, penetration testing, incident response planning, or security training.
Agreement and Engagement: Enter into a service agreement with Cyberlinx Security detailing the scope, timeline, and deliverables of the chosen services.
Implementation: Work closely with Cyberlinx Security's team throughout the implementation phase, providing necessary access and information as required.
By following these steps, individuals and organizations can access Cyberlinx Security's comprehensive suite of services and strengthen their cyber defenses effectively.

12 PUBLIC INVOLVEMENT IN THE FORMULATION OF POLICY OR THE EXERCISE OF POWERS OR PERFORMANCE OF DUTIES BY CYBERLINX SECURITY

The public can submit formal requests to the Chief Information Officer Of Cyberlinx Security

13 PROCESSING OF PERSONAL INFORMATION

13.1 Purpose of Processing

The diligent process of responding to requests for quotes and tenders, coupled with the precise execution and timely delivery of the comprehensive suite of cyber security services provided by Cyberlinx Security, ensures that clients receive tailored solutions that meet their specific needs, guaranteeing robust protection against modern digital threats and fostering a secure digital environment.

13.2 Description of the categories of Data Subjects and of the information or categories of information relating thereto

13.3 Information Collection

In the event that personal information is collected from the information subject, with his/her consent, the Company commits to be transparent in its processing of personal information and provides the information subject with the following:

- The Company’s identity and the contact details of the Information Officer (hereinafter referred to as the IO) and any information protection representatives.
- The purpose(s) including legal basis, for the intended processing of personal information;
- Where relevant, Cyberlinx’s legitimate interests that provide the legal basis for the processing of the information;
- Potential recipients of personal information;
- Any information regarding the intention to disclose personal information to third parties and whether it is transferred outside South Africa. In such circumstances, the Company will provide information on the safeguards in place and how the information subject can also obtain a copy of these safeguards
- Any information on website technologies used to collect personal information about the information subject;
- Any information required to demonstrate that the processing is fair and transparent which includes but is not limited to information on the information subjects' rights to access, right to lodge a complaint, right to withdraw consent, information on why processing is necessary if it’s a statutory or contractual requirement, any automated decision making (profiling) and any other further purpose to the processing other than that originally collected for.

13.4 What personal information we collect at Cyberlinx from our employees

For the purpose of employment, employees are required to provide consent to the Company to process their Personal Information Form (CX-HRF-FRM-001) for onboarding, payroll, provident fund and employment related matters which includes but is not limited to the following:

- Full Names and Surname; and
- Maiden Name where applicable; and
- ID Number; and
- Marital Status; and
- Gender; and
- Personal Email and Cellular Phone number; and
- Address (unit number, complex, street number, street name, suburb, town, province and postal code; and
- Postal address; and
- Tax reference number; and
- Work permit (if applicable); and
- Spouse's / Life Partner details; and
- Banking details

13.5 Processing of Personal Information

The processing of information includes collecting, receiving, recording, organising, retrieving or using such information or disseminating, distributing or making such personal information available.

13.6 Personal Information of Customers

13.6.1 Information Collection

We collect and process customer personal information mainly to contact the customer for the purposes of understanding his/her requirements and to deliver services accordingly.

Cyberlinx will collect information directly from the customer where the customer provides the Company with his/her personal details. Where possible, the Company will inform the customer what information is required to be provided and what information will be optional.

13.6.2 Website Information (Customers)

Website usage information may be collected using "cookies" which allows us to collect standard internet visitor usage.

For the purpose of Spam Detection, the following will be used:

- IP Address
- Browser user agent string.

For the purpose of profiles in the comments section:

- Anonymized string created from the customer's email address (also called a hash);
- This will be shared to the Gravatar service in order to auto populate the customer's Avatar and related details (refer to https://autmoattic.com/privacy/;
- Media can be manually uploaded to populate profile pictures. These images will only be utilised for the customer's profile and will not be processed further.

13.6.3 Cookies

Cyberlinx uses cookies to personalise content and advertisements to provide social media features and to analyse Cyberlinx's traffic. The Company shares information about the use of our site with our social media, advertising and analytics partners who may combine it with other information that the customer has provided to them or that they've collected from the customer's use of their services.

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

The following table outlines the categories and breakdown of personal information processed and who may be a recipient of this PII in terms of this Act.

Categories & Breakdown of Personal Information processed	Recipients or Categories of Recipients
Customer Information, restricted to the following: Name; Email address; Company Designation & Job Title Contact Number Place of work or Business Address	**Vendor Partner:** (for the purposes of concluding a technology sale or service)
Some of the following Employee Information: Name Identity Number Business email address Designation & Job Title Contact Number Place of work. Redacted CV or BIO Qualifications	**Vendor Partner**: (for partnership compliance status), **Customers (**in response to tenders requesting qualifications or; In the delivery of a service or implementation for the customer)
Some of the following Employee Information: Name Identity Number Business email address Private email address Home address Designation & Job Title Contact Number Place of work Qualifications	**Company Insurance, Medical Aid, & Pension Fund**

13.8 Planned transborder flows of personal information

N/A

13.9 General Description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information

- A Firewall is implemented at the company head office.
- Data Loss Prevention Technology implemented through the company cloud platforms.
- EDR and Antivirus Technology has been deployed throughout the organisation

- Encryption has been enforced and enabled throughout the organisation
- Multi-Factor Authentication is enforced throughout the organisation.
- All staff engage in mandatory security awareness training on a regular basis.

14 AVAILABILITY OF THE MANUAL

14.1 A copy of this Manual or the updated version thereof, is also available as follows:

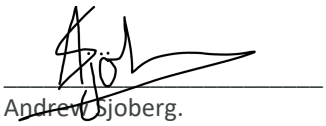
- To any person upon request and upon the payment of a reasonable prescribed fee; and
- to the Information Regulator upon request.

14.2 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.

15 UPDATING OF THE MANUAL

Cyberlinx Security will, if necessary, update and publish this Manual annually.

Issued By:



Andrew Sjoberg.
Information Officer.