WWW.CYBERRES.CO.ZA

CYBER
RESILIENCE
AFRICA

PRIVACY POLICY

CRA.PO.06

Document Owner:	Managing Director
Document Version:	5
Creation Date:	July 2022

Table of Contents

1. Document Control

1.1. Version Control

Document Name	Privacy Policy
Document No. and Version	CRA.PO.06 Version 5
Next Review Date	June 2028
Date Last Reviewed	June 2026
Document Owner	Managing Director (Privacy Officer)

1.2. Updates to this document

This document will be reviewed biennially, or sooner where required, to ensure it remains accurate, risk-aligned, and consistent with Cyber Resilience's business environment, technology landscape, legal obligations, and Information Security Management System (ISMS).

An out-of-cycle review may be triggered by, but is not limited to:

- changes to applicable legislation, regulatory, or contractual requirements;
- material changes to organisational structure, business operations, or services;
- significant changes to systems, technologies, or security controls;
- relevant audit findings, security incidents, or identified control weaknesses; or
- updates to related policies, standards, or procedures

1.3. Change History

The record below must be completed by the person making the amendment(s). Each new version of this document will include an updated version number and issue date.

Where a scheduled review is conducted and no material changes are made, the issue date will be updated while the version number remains unchanged. Formatting or cosmetic changes that do not affect the meaning, intent, or control requirements of the document do not require a new version number or issue date.

Version	Issue Date	Pages Amended	Amended by
1.0	07/2022	All – Policy created	P. Cianfanelli
2.0	10/2023	Template update	P. Cianfanelli
3.0	01/2025	Website and business data sections added.	J. Stols

Version	Issue Date	Pages Amended	Amended by
4.0	01/2026	POPIA and GDPR alignment; governance and transparency enhancements.	J. Stols
5.0	06/2026	Added section 6.14 (special personal information and prior authorisation); corrected document cross-references.	J. Stols

1.4. Distribution

Once approved, this document will be made available to all relevant individuals and will be accessible to Cyber Resilience personnel via the company's approved document repository or shared drive.

Issued To	Issue Date	Position/s
www.f-si.co.za and all employees	08/2022	All
www.f-si.co.za and all employees	01/2024	All
www.f-si.co.za and all employees	02/2025	All
www.cyberres.co.za and all employees	01/2026	All
www.cyberres.co.za and all employees	06/2026	All

2. Purpose

This Privacy Policy describes how Cyber Resilience, as a responsible party and data controller, lawfully collects, uses, stores, shares, and protects personal information.

The policy provides transparency regarding the processing of personal information in accordance with the Protection of Personal Information Act, 4 of 2013 (POPIA), and, where applicable, the General Data Protection Regulation (EU) 2016/679 (GDPR). It explains how personal information is processed when individuals interact with Cyber Resilience through its website, during business operations, or while providing services.

3. Scope

This policy applies to all personal information processed by Cyber Resilience, including information relating to clients, prospective clients, website visitors, employees, contractors, suppliers, and other third parties.

The policy applies to all processing activities performed by Cyber Resilience, whether conducted electronically, manually, or through third-party service providers, and covers both internal governance and public-facing transparency requirements.

4. Roles and Responsibilities

Role	Responsibility
Privacy Officer	Overall accountability for privacy compliance; oversight of personal information processing; handling data subject requests; liaison with regulators; oversight of third-party privacy risk; monitoring and reporting on compliance.
Directors	Ensuring organisational compliance with privacy obligations and allocating appropriate resources.
Employees and Contractors	Processing personal information in accordance with this policy and reporting privacy risks or incidents.
Technical Director	Oversight of technical safeguards, international data transfers, and privacy-related technology controls.

5. References

- Protection of Personal Information Act, 4 of 2013
- General Data Protection Regulation (EU) 2016/679
- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- CRA.MA.02 PAIA Manual
- CRA.ST.01 Information Handling Standard
- CRA.ST.02 Record Retention Standard

6. Policy Statement

6.1. Privacy Objectives

Cyber Resilience's privacy objectives are to:

6.1.1. Protect the confidentiality, integrity, and availability of personal information.

6.1.2. Ensure transparency regarding how personal information is collected and used.

6.1.3. Enable data subjects to exercise their rights effectively.

6.1.4. Ensure compliance with POPIA and, where applicable, GDPR requirements.

6.1.5. Embed privacy considerations into business operations, systems, and decision-making.

6.2. Commitment to Privacy Compliance

Cyber Resilience is committed to processing personal information lawfully, fairly, and transparently. The organisation ensures that personal information is collected and used only

for legitimate business purposes, protected against unauthorised access or misuse, and processed in accordance with applicable privacy legislation.

This policy supports Cyber Resilience's accountability obligations and forms part of the organisation's broader governance framework.

6.3. Categories of Personal Information Processed

Cyber Resilience may process personal information including (as applicable to the context and relationship): names and surnames, contact details, employer and role information, contractual and billing-related information, recruitment and employment information, and other information required to provide services or meet legal or contractual obligations.

Where individuals interact with Cyber Resilience digitally (including via the website), Cyber Resilience may also process **technical and usage-related information**, which may include IP address, approximate location (derived from IP), device type and identifiers, operating system, browser type and version, referral pages, pages viewed, date/time of access, and diagnostic or security-related logs.

6.4. Lawful Basis for Processing

Personal information is processed only where a lawful basis exists. Depending on the processing activity, this may include performance of a contract, legal obligation, legitimate interests (where not overridden by the rights of the data subject), or consent.

Where consent is relied upon, it will be obtained in a clear and informed manner and may be withdrawn at any time.

6.5. Purpose Limitation and Minimality

Cyber Resilience processes personal information only for defined and lawful purposes and limits collection to information that is adequate, relevant, and not excessive for the intended purpose.

6.6. Accuracy and Currency

Where Cyber Resilience reasonably relies on personal information to deliver services, meet legal obligations, or maintain operational records, it will take reasonable steps to ensure information is accurate and updated where required. Data subjects may request correction or updating of their information.

6.7. Access Control and Confidentiality

Access to personal information is restricted to authorised individuals who require access to perform their duties. Personnel and contractors are required to maintain confidentiality and comply with Cyber Resilience information handling and security requirements.

6.8. Information Security Safeguards

Cyber Resilience implements appropriate technical and organisational measures to protect personal information against loss, unauthorised access, disclosure, alteration, or destruction, aligned to its Information Security Management System and applicable standards.

6.9. Retention, De-identification, and Deletion

Personal information is retained only for as long as necessary to fulfil the relevant purpose, to comply with legal or contractual obligations, or to resolve disputes. Once retention periods expire, personal information is securely deleted, destroyed, or de-identified in accordance with Cyber Resilience retention and information handling requirements.

6.10. Sharing of Personal Information and Third-Party Processing

Cyber Resilience may share personal information with third parties only where there is a lawful basis and a legitimate business requirement. Where third parties process personal information on behalf of Cyber Resilience, Cyber Resilience requires appropriate contractual safeguards and confidentiality obligations and applies a risk-based approach to supplier oversight for privacy and security.

Personal information may also be disclosed where required by law, court order, regulatory request, or lawful authority request.

6.11. Cross-Border Transfers

Cyber Resilience may process or store personal information using systems or service providers that operate across jurisdictions. Where cross-border transfer occurs, Cyber Resilience applies appropriate safeguards consistent with applicable legal requirements and ensures reasonable assurance that personal information will continue to be protected.

6.12. Marketing and Unsolicited Communications

Where Cyber Resilience sends direct marketing communications, it will do so in a manner consistent with applicable requirements, including providing recipients with a reasonable mechanism to opt out of future marketing communications. Opt-out requests will be implemented within a reasonable period and without charge.

6.13. Automated Decision-Making and Profiling

Cyber Resilience does not make decisions that produce legal effects or similarly significant consequences for individuals based solely on automated processing, including profiling, without meaningful human involvement.

Where automated processing tools are used to support operational, security, or analytical activities (for example, for threat detection, website analytics, fraud detection, or service optimisation), such processing is implemented as a support mechanism and does not independently determine outcomes that materially affect data subjects.

If Cyber Resilience were to introduce automated decision-making processes that may have legal or substantial consequences for individuals, the organisation will:

6.13.1. Ensure that such processing is supported by an appropriate lawful basis under applicable privacy legislation.

6.13.2. Provide clear notification to affected data subjects regarding the existence of automated decision-making, including meaningful information about the logic involved and the potential consequences.

6.13.3. Ensure that decisions are subject to meaningful human review and intervention prior to finalisation.

6.13.4. Provide data subjects with the right to request human intervention, to express their point of view, and to contest the decision, where applicable.

Cyber Resilience will assess any proposed automated processing activities as part of its privacy governance and risk management processes to ensure alignment with POPIA, GDPR (where applicable), and internal information security requirements.

6.14. Special Personal Information and Prior Authorisation

Cyber Resilience recognises that certain categories of personal information are classified as **special personal information** under section 26 of POPIA, including information concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, and information relating to criminal behaviour to the extent that it relates to the alleged commission of an offence or to proceedings in respect of an offence.

Cyber Resilience does not process special personal information unless a lawful basis exists under section 27 of POPIA — including where the data subject has consented, where processing is necessary for the establishment, exercise, or defence of a right or obligation in law, or where another statutory authorisation applies.

In the course of delivering forensic, investigative, or security services, Cyber Resilience may process information relating to criminal behaviour or alleged offences on behalf of clients. Where such processing falls within the circumstances described in section 57 of POPIA — including the processing of information concerning criminal behaviour or unlawful or objectionable conduct on behalf of third parties — Cyber Resilience will obtain prior authorisation from the Information Regulator before commencing that processing and will not commence such processing until the required authorisation has been granted.

Where special personal information is processed, Cyber Resilience applies enhanced safeguards, including restricted access on a strict need-to-know basis, additional confidentiality controls, and secure handling and disposal in accordance with its information security and records retention requirements.

7. PI collected via the website

7.1. Cookies and Similar Technologies

Cyber Resilience uses cookies and similar technologies to support website functionality, improve user experience, and understand website performance. Cookies may be session-based (deleted when the browser is closed) or persistent (retained for a defined period).

Where applicable, Cyber Resilience uses cookies for purposes such as enabling core website functionality, storing website preferences, and measuring website usage trends. Users may manage cookie preferences through browser settings or consent tools where implemented. Disabling certain cookies may impact website functionality.

7.2. Website Usage and Technical Data

When users access the website, Cyber Resilience may collect technical and usage data automatically generated by the interaction, including IP address, device identifiers, browser type/version, pages visited, referring URLs, and timestamps. This information is used for security monitoring, performance analysis, and improving website functionality.

7.3. Contact Forms and Enquiries

Personal information submitted via website contact forms or email enquiries is used to respond to enquiries, provide requested information, and manage follow-up communication. This information is not shared without a lawful basis.

7.4. Job Application Information

Personal information submitted for recruitment purposes is processed for evaluating applications and managing recruitment activities. Recruitment information is retained for a limited period unless further retention is required by law or legitimate business needs.

7.5. Links to Other Websites and Embedded Content

The Cyber Resilience website may contain links to third-party websites or embedded content. Cyber Resilience is not responsible for the privacy practices of third parties, and users are encouraged to review third-party privacy policies where applicable.

8. PI Collected to Facilitate Business Operations

8.1. What Personal Information Is Collected

This may include names, contact details, professional information, contractual information, billing-related information, supplier information, and other data necessary to provide services, manage relationships, or meet legal obligations.

8.2. How Personal Information Is Collected

Personal information is collected directly from data subjects, from client organisations (where relevant to service delivery), and through lawful third-party sources where applicable.

8.3. How Personal Information Is Used

Personal information is used to:

- Deliver and manage services
- Manage contractual relationships and client engagement
- Communicate with stakeholders
- Meet legal and regulatory obligations
- Maintain operational records and governance evidence
- Support security monitoring and incident management where relevant to protecting information and systems

8.4. Storage and Retention of Personal Information

Personal information is stored securely using appropriate safeguards and retained in accordance with defined retention schedules.

8.5. Sharing of Personal Information with Third Parties

Personal information is shared only where necessary for service delivery, operational support, legal compliance, or other lawful purposes. Cyber Resilience applies a governance-based approach to third-party sharing, including confidentiality obligations and appropriate safeguards, and limits sharing to the minimum necessary.

8.6. Personal Information of Minors

Cyber Resilience processes personal information relating to minors only where legally permitted and strictly necessary, such as in the context of forensic or investigative services. Where required, appropriate authority or consent is obtained, access is restricted, and enhanced safeguards are applied to protect the rights and interests of minors.

9. Data Subject Rights

Data subjects have the right to:

- Access their personal information
- Request correction or deletion
- Object to or restrict processing
- Withdraw consent where applicable
- Lodge a complaint with the Information Regulator

10.Contact Details of the Privacy Officer

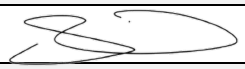
Name and Surname	Jeanine Stols
Position	Managing Director
Email	jeanine@cyberres.co.za
Contact Number	087 265 3683

11.Breaches of this Policy

Breaches of this policy will be managed in accordance with Cyber Resilience's disciplinary and corrective action procedures and may result in corrective measures, disciplinary action, removal of access privileges, or other appropriate sanctions.

In the case of contractors, consultants, or other third parties, breaches may result in suspension or termination of services, removal of access to systems or information, contractual remedies, or legal action where applicable.

12.Policy Approval

Authorised by:	Director: Jeanine Stols		19 June 2026
		Signature	Date
	Director: Seyton Hayes		19 June 2026
		Signature	Date
	Director: Warren Bonheim		19 June 2026
		Signature	Date

13.Policy Definitions

Term	Definition
Personal Information (PI)	Information relating to an identifiable, living natural person, and where applicable, an identifiable existing juristic person, including but not limited to contact details, identification information, employment information, online identifiers, or any information as defined under the Protection of Personal Information Act, 4 of 2013.

Term	Definition
Personally Identifiable Information (PII)	Any information that can be used to identify a specific individual, either directly or indirectly, including personal information as defined under POPIA and personal data as defined under the GDPR.
Data Subject	The natural or juristic person to whom personal information relates. Under GDPR, this refers to an identified or identifiable natural person.
Data Controller	The entity which determines the purposes and means of processing personal data, as defined under the GDPR. For the purposes of this policy, Cyber Resilience acts as the responsible party and, where applicable, the data controller.
Data Processor	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller, as defined under the GDPR.
Operator	A person or organisation that processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that responsible party, as defined under POPIA.
Responsible Party	The organisation or public body which, alone or in conjunction with others, determines the purpose of and means for processing personal information, as defined under POPIA.
Consent	Any voluntary, specific, informed, and unambiguous indication of a data subject's wishes by which they agree to the processing of their personal information.
Processing	Any operation or activity concerning personal information, whether automated or manual, including collection, receipt, recording, organisation, storage, updating, retrieval, consultation, use, dissemination, alignment, restriction, erasure, or destruction.
Breach	A security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information.
Minor	A natural person under the age of 18 years, as recognised under South African law.
Usage Data	Technical information automatically generated by interactions with the website or systems, such as IP address, device identifiers, browser type/version, and pages viewed.