

DATA PROTECTION POLICY

CONTENTS

A.	DATA PROTECTION POLICY	1
	POLICY OBJECTIVES	1
	PURPOSE	1
	SCOPE	1
	APPLICATION	1
	DEFINITIONS	2
	ROLES AND RESPONSIBILITIES	2
	PRINCIPLES OF DATA PROTECTION	3
B.	CONSENT MECHANISMS	5
C.	OPERATOR RESPONSIBILITIES.....	6
D.	CLEAN DESK POLICY	7
E.	PHYSICAL SECURITY	8
F.	INFORMATION CLASSIFICATION.....	10
G.	DATA RETENTION AND DESTRUCTION	11
	SCHEDULE 1.....	13
H.	VENDOR MANAGEMENT	14
I.	BREACH MANAGEMENT.....	14
J.	POLICY COMPLIANCE AND REVIEW	15
K.	POLICY BREACH	15
L.	ENFORCEMENT	15

A. DATA PROTECTION POLICY

POLICY OBJECTIVES

This policy applies to all member companies of the "Eezispace Self Storage (Pty) Ltd".

At Eezispace Self Storage, we are committed to protecting the personal information of all stakeholders including our employees, clients, candidates, and service providers. As a registered Self Storage facility, we understand that the secure and lawful handling of personal information is not only a legal obligation under the Protection of Personal Information Act (POPIA), but also essential to maintaining the trust placed in us by our partners and the employees we manage.

This policy outlines how Eezispace Self Storage Services collects, uses, processes, and protects personal information in accordance with POPIA. It applies to all data subjects whose personal information we hold, within the self storage business operations.

PURPOSE

The purpose of this policy is to outline how Eezispace Self Storage Services lawfully collects, processes, stores, and protects personal information in accordance with POPIA. As a self storage facility, Eezispace Self Storage Services processes personal data relating to employees, independent contractors, clients, and service providers.

This policy serves to ensure that the rights of data subjects are upheld and that Eezispace Self Storage Services complies with POPIA's conditions for lawful processing of personal information.

SCOPE

This policy applies to all personal information processed by Eezispace Self Storage Services in the course of conducting business operations. This includes, but is not limited to:

- Employee personal information.
- Client business and contact information
- Service provider and supplier information
- Data collected via our website <https://Eezispace.co.za> or through digital platforms and email correspondence
- Information processed for clients self storage needs.

The policy also governs internal processing activities within Eezispace Self Storage Services, including staff access to and handling of personal data for operational or administrative purposes.

APPLICATION

This policy applies to:

- All Eezispace Self Storage Services employees and contracted personnel

- Third-party operators who process personal information on behalf of Eezispace Self Storage Services
- Clients, candidates, and suppliers engaging with Eezispace Self Storage Services
- Any party whose personal information is shared with, collected by, or processed through Eezispace Self Storage Services' systems, whether digital, paper-based or through verbal interactions

All users and stakeholders are expected to adhere to the principles outlined herein and participate in maintaining data privacy compliance across all operational areas.

DEFINITIONS

To ensure clarity and consistent understanding throughout this policy, the following definitions are applicable:

- 1) **Data Subject:** The individual or entity to whom personal information relates, such as employees, candidates, clients, or service providers.
- 2) **Personal Information:** Any information relating to an identifiable, living natural person or existing juristic person, including but not limited to names, contact details, identity numbers, employment history, and opinions.
- 3) **Special Personal Information:** Information relating to race, health, biometric data, criminal records, religious or philosophical beliefs, and trade union membership.
- 4) **Processing:** Any operation or activity concerning personal information, whether automated or not, including collection, storage, use, dissemination, or destruction.
- 5) **Responsible Party:** Eezispace Self Storage Services, who determines the purpose and means for processing personal information.
- 6) **Operator:** A third party who processes personal information on behalf of Eezispace Self Storage Services under a written contract or mandate.
- 7) **Information Officer:** The individual appointed in terms of POPIA to ensure compliance within Eezispace Self Storage Services, supported by any designated Deputy Information Officers (DIOs).
- 8) **Consent:** Voluntary, specific, and informed expression of will by a data subject agreeing to the processing of their personal information.
- 9) **Data Breach:** Any event where personal information is accessed, disclosed, or destroyed in an unauthorised manner.

ROLES AND RESPONSIBILITIES

Responsibilities of Senior Management

Senior Management plays a pivotal leadership role in upholding data protection by:

- a) Ensuring appropriate governance structures, resources, and controls are in place for compliance with POPIA.
- b) Promoting a culture of privacy and data responsibility across all departments and regions.
- c) Supporting all data protection initiatives and driving accountability from top to bottom.
- d) Allocating resources (financial, human, and technological) necessary for effective data protection.
- e) Enforcing the Clean Desk Policy to minimise unauthorised access to sensitive information.

- f) Overseeing implementation of robust physical and IT security controls, including access management and surveillance.
- g) Approving and regularly reviewing data classification frameworks to ensure proper identification and safeguarding of information assets.
- h) Endorsing and reviewing data retention and destruction schedules to ensure legal and ethical compliance.
- i) Supporting the Information Officer through leadership buy-in, periodic review of compliance progress, and accountability enforcement.

Responsibilities of the Information Officer

The Information Officer acts as the compliance custodian and is responsible for:

- a) Driving the implementation of Eezispace Self Storage Services' POPIA compliance strategy.
- b) Monitoring compliance with data protection laws and internal policies.
- c) Providing ongoing guidance, training, and awareness to internal stakeholders.
- d) Responding to data subject requests and ensuring their rights are respected.
- e) Serving as the main liaison with regulatory bodies and data subjects.
- f) Conducting audits to measure the effectiveness of data protection practices.
- g) Advising on and reviewing security protocols in both physical and digital environments.
- h) Overseeing information classification processes and ensuring their proper application.
- i) Ensuring data retention and destruction practices are implemented, maintained, and reviewed regularly.
- j) Staying abreast of regulatory updates and amending policies as needed.

Responsibilities of All Employees

All employees, including contractors and temporary staff, are required to:

- a) Adhere to this POPIA Policy and all associated compliance requirements.
- b) Handle all personal information with diligence, confidentiality, and care.
- c) Keep physical and digital workspaces organised to avoid unintentional data exposure.
- d) Report suspected data breaches or concerns immediately to the Information Officer.
- e) Obtain consent from data subjects where applicable and explain processing activities transparently.
- f) Process personal information only when authorised and within the purpose specified.
- g) Participate in ongoing data protection training and awareness initiatives.
- h) Assist in enforcing physical security measures (e.g., locking away documents, following visitor protocols).
- i) Follow correct procedures for data storage, retention, and destruction.
- j) Maintain awareness of the company's data retention timelines and their application in daily responsibilities.

PRINCIPLES OF DATA PROTECTION

Lawfulness, Fairness and Transparency

Eezispace Self Storage Services ensures that all personal information is processed:

- **Lawfully:** In full compliance with applicable laws and regulatory requirements.
- **Fairly:** With due regard for the interests, rights, and expectations of all data subjects, including employees, candidates, clients, and service providers.
- **Transparently:** Individuals are informed of the purpose and scope of personal data collection and processing, primarily through contracts, consent forms, and privacy notices.

For example, during recruitment or onboarding, individuals are notified of how their data will be used, such as for placement, payroll, and compliance reporting.

Purpose Limitation and Data Minimisation

Personal information is collected and processed solely for legitimate, specific, and explicitly defined purposes related to Eezispace Self Storage Services' operations.

Employees and contractors must ensure:

- Only the minimum required personal information is collected.
- Information is not reused for unrelated purposes unless lawful justification or further consent is obtained.

Accuracy and Storage Limitation

Eezispace Self Storage Services is committed to maintaining accurate and complete personal information. It is the responsibility of both staff and data subjects to ensure that personal details are up to date and corrected where necessary.

- Personal data must be reviewed and updated regularly.
- Information is retained only for as long as necessary to fulfil its original purpose or to meet statutory obligations. Once retention periods expire, data is securely destroyed in accordance with the company's Data Retention Policy.

Security and Confidentiality

Robust technical, physical, and organisational measures are in place to protect personal data from loss, misuse, unauthorised access, disclosure, or destruction.

Security controls include:

- Technical safeguards such as encryption, password protection, and access restrictions.
- Physical safeguards such as controlled office access and document storage procedures.
- Organisational safeguards including mandatory training, Clean Desk Policy enforcement, and breach reporting protocols.

All staff members are required to handle personal information with the highest level of confidentiality and only disclose such information when lawfully authorised.

Data Subject Rights

Eezispace Self Storage Services recognises the rights of data subjects as follows:

Access and Rectification

- Individuals have the right to access their personal information and request corrections or updates where data is inaccurate or incomplete.
- Eezispace Self Storage Services is committed to responding to these requests in a timely and compliant manner.

Erasure and Restriction

- Data subjects may request the deletion or restriction of their personal data under certain conditions, including where it is no longer necessary for processing or where consent has been withdrawn.
- All such requests will be evaluated with respect to applicable legal and contractual data retention obligations.

Objection and Data Portability

- Data subjects may object to the processing of their personal information, particularly in relation to direct marketing.
- Where applicable, and technically feasible, individuals may request the transfer of their personal data to another responsible party.

Eezispace Self Storage Services will respond to these requests in accordance with POPIA and internal procedures to ensure the rights of individuals are upheld consistently and lawfully.

B. CONSENT MECHANISMS

Eezispace Self Storage Services recognises the importance of obtaining and managing consent in accordance with POPIA. Consent forms part of the legal basis for processing personal information, particularly in employment-related activities and client engagements.

Obtaining Consent

- Consent must be **voluntary, specific, informed, and unambiguous**.
- It must be obtained in writing or via secure digital platforms where appropriate.
- Eezispace Self Storage Services obtains consent from:
 - **Clients and suppliers** via service agreements and terms of engagement.
 - **Third-party contractors or operators** through contractual clauses and service-level agreements.

Consent for Special Personal Information

Where special personal information is processed—such as health status, biometric data, or union affiliation—explicit consent must be obtained and documented, except where such processing is legally required (e.g., for B-BBEE, health surveillance, or payroll tax submissions).

Withdrawal of Consent

- Data subjects may withdraw their consent at any time.
- Eezispace Self Storage Services provides a structured process to receive, evaluate, and act on withdrawal requests.
- The withdrawal of consent does not affect the lawfulness of processing prior to the withdrawal and may not override legal or contractual retention requirements.

C. OPERATOR RESPONSIBILITIES

Eezispace Self Storage Services makes use of external service providers (operators) in areas such as IT support, payroll platforms, and marketing. These operators process personal information on behalf of Eezispace Self Storage Services and must do so in full compliance with POPIA.

Operator Agreements

- All operators must sign formal written agreements that set out:
 - The purpose and scope of processing.
 - Confidentiality obligations.
 - Security and data protection measures required.
 - Procedures for reporting data breaches.
- Eezispace Self Storage Services ensures that these agreements include:
 - Prohibition against unauthorised disclosure or further processing.
 - A duty to return or destroy data upon termination of the contract.

Oversight and Accountability

Eezispace Self Storage Services, as the responsible party, retains full accountability for the data processed by operators. As such:

- Due diligence is conducted before appointing any operator.
- Periodic reviews and audits are carried out to assess operator compliance.
- Operators are required to report any data breach, security concern, or access request related to the personal information they process.

Transborder Information Flow

- If personal information is transferred to an operator in a foreign country (e.g., cloud hosting or group-level IT support), Eezispace Self Storage Services ensures that:
 - The operator is subject to data protection laws or agreements that provide an adequate level of protection.

- Data subjects are informed of the nature and purpose of such transfers, where applicable.

D. CLEAN DESK POLICY

As a company handling large volumes of personal and confidential data related to candidates, employees, clients, and service providers, Eezispace Self Storage Services enforces a strict Clean Desk Policy to prevent unauthorised access to sensitive information.

All employees are required to secure documents and devices containing personal or confidential information in designated lockable cabinets, drawers, or secure digital platforms when not in use—particularly when leaving their desks unattended or at the end of each workday.

No personal or confidential information may be left exposed in open workspaces, meeting rooms, or any public areas. This includes printed CVs, employment contracts, payroll records, or client correspondence.

Keys, access cards, and authentication devices used to access restricted areas or sensitive systems must be kept secure and never left unattended or openly accessible.

Overview

This policy is an essential control to mitigate the risk of information leakage, accidental exposure, or unauthorised access to personal and confidential data.

As a POPIA-aligned and ISO-compliant measure, the Clean Desk Policy also enhances staff awareness of data protection responsibilities, supporting the company's overall information security framework.

Scope

This policy applies to all Eezispace Self Storage Services employees, contractors, and consultants operating at:

- Eezispace Self Storage Services' regional offices or head office locations
- Home or remote work environments under company authorisation
- On-site client premises where employees represent Eezispace Self Storage Services and handle sensitive information

It includes all physical workstations, mobile devices, company-issued laptops, personal computers used for work purposes, and any paper-based or electronic documents under Eezispace Self Storage Services' control.

Policy Statement

Employees must adhere to the following clean desk and secure handling procedures:

- All paper-based personal or confidential documents must be stored securely when not in use.
- Desks and meeting spaces must be cleared of notes, reports, and printouts containing sensitive information at the end of each day or prior to extended absence.
- Workstations must be locked when left unattended.
- All computers and devices must be fully shut down at the end of the working day.
- Filing cabinets containing employee or client information must be closed and locked when unattended.
- Access tools (keys, cards, etc.) must not be left in accessible areas.
- Passwords must never be stored on desks or shared in visible locations.
- Whiteboards in meeting rooms must be cleared of sensitive notes after use.

Secure Disposal and Clearing Procedures

- a) All confidential documents must be disposed of using the designated secure disposal methods, such as cross-cut shredders or locked disposal bins, available at all Eezispace Self Storage Services offices.
- b) Disposal bins must be cleared regularly, and the contents securely destroyed in accordance with POPIA-aligned disposal procedures to prevent reconstruction or misuse.
- c) Printed documents containing personal or confidential data (e.g., Contracts, ID copies) must be removed from printers immediately after printing.
- d) A regular printer clearance routine must be implemented, especially in shared printer environments, to prevent unauthorised viewing or pickup of documents.

E. PHYSICAL SECURITY

Physical Access

- Access to areas where personal information is processed or stored—such as client service zones—is strictly limited to authorised personnel only. This restriction supports the confidentiality and integrity of all sensitive personal and client data handled by Eezispace Self Storage Services.
- Where applicable, electronic access control systems such as badges, biometric readers, keys, or swipe cards must be used to monitor and manage access to secure areas. These systems must ensure both entry and exit are tracked and auditable.
- Employees are not permitted to share access credentials under any circumstances. Any loss or theft of keys, cards, or credentials must be reported immediately so that they can be deactivated or replaced, ensuring access is restricted to authorised users only.

Visitor Access

- Visitors to any Eezispace Self Storage Services location must be accompanied at all times by an authorised employee. This includes clients, auditors, IT vendors, or maintenance service providers. Escorting visitors ensures that no unauthorised access to personal or client information occurs.

- All visitors must sign in and out using a visitor log or electronic register and be issued temporary visitor identification where available.
- Contractors or third-party service providers must be granted access only to the areas necessary to perform their duties. Access beyond their immediate operational scope is not permitted unless explicitly approved and supervised.

Remote Access

- For employees or consultants accessing company systems remotely (e.g. client onboarding), secure authentication protocols must be enforced. This includes the use of Virtual Private Networks (VPNs), strong password policies, and Multi-Factor Authentication (MFA).
- Remote access must be limited to authorised users and closely monitored to prevent unauthorised exposure of personal information.

Surveillance and Monitoring

Video Surveillance

- Where implemented, video surveillance is used to monitor the premises for unauthorised entry, protect personnel and assets, and support investigations of security-related incidents.
- Cameras must be positioned to monitor sensitive areas without violating the privacy rights of employees or visitors.
- Footage must be securely stored and only accessible to authorised individuals. Retention of surveillance footage must comply with POPIA and relevant regulatory guidelines.

Access Logs

- Physical access to areas where personal or confidential information is stored such as filing rooms, client contract areas must be logged where feasible. Logs should record who accessed the area, the time of access, and the duration.
- Regular reviews of access logs must be conducted to detect anomalies or any potential unauthorised access.

Physical Security Measures

Eezispace Self Storage Services must implement layered security measures to ensure physical protection of assets and personal information across all office locations.

This includes:

- Security barriers or checkpoints at entrance points, with limited entry based on staff authorisation.

- Adequate exterior and perimeter lighting, particularly in after-hours operational zones.
- Intrusion detection systems and alarms in areas where sensitive documentation or hardware is stored.
- A documented response plan for security alerts or breaches, including emergency contacts and designated security responders.
- Lockable cabinets, safes, or restricted-access rooms for physical files and documents that contain personal information.
- Employee responsibility for securing their workstations and filing systems when unattended.
- Portable devices such as laptops or tablets that contain personal data must be locked away when not in use.
- Any loss or theft of devices or physical files must be reported immediately to the designated compliance or IT authority to assess risk and initiate containment measures.

F. INFORMATION CLASSIFICATION

Eezispace Self Storage Services acknowledges the vital importance of systematically classifying the information it processes, stores, and manages in order to protect the confidentiality, integrity, and availability of personal and business-critical data.

The company handles large volumes of personal information related to employees, clients, service providers, and internal stakeholders. Given the sensitive nature of this data especially within functions such as self storage, it is essential to apply appropriate levels of protection based on a structured classification approach.

Information assets are classified according to their sensitivity and potential impact on Eezispace Self Storage Services' operations, legal obligations, client relationships, and brand reputation. Factors considered include:

- The degree of confidentiality required
- The potential risk of unauthorised access or disclosure
- Legal and regulatory requirements under POPIA, CPA, BCEA, and sector-specific regulations
- The operational criticality of the information
- The reputational or financial damage that could result from compromise or misuse

The Eezispace Self Storage classification level determines how information is accessed, stored, shared, transmitted, and disposed of. Security measures and handling protocols are calibrated based on the classification level to ensure proportional protection and compliance.

Eezispace Self Storage Services commits to regularly reviewing its information classification framework to reflect:

- Changes in business operations and services
- Updates in legislative or regulatory requirements
- New or emerging data protection risks
- Evolving expectations of clients, regulatory bodies, and business partners

This ensures that all personal, operational, and client information is consistently protected in line with risk exposure, compliance needs, and organisational priorities.

A supporting Information Classification Table provides specific criteria for classification levels (e.g., Public, Internal, Confidential, and Restricted), along with their associated access controls, storage rules, and handling procedures. All employees are required to apply these guidelines consistently and are trained on classification obligations as part of their compliance responsibilities.

Classification Level	Description	Examples	Access Controls	Storage & Handling
Public	Information intended for public access. Disclosure poses no risk to the company or data subjects.	• Company website content • Marketing brochures • Published service offerings	No restrictions	Can be stored on public platforms (e.g., website). No encryption or access restrictions required.
Internal	Operational or administrative information that is not public but poses minimal risk if disclosed.	• Internal SOPs • Staff rosters • Non-sensitive meeting minutes	Limited to employees and authorised consultants	Stored on internal drives or cloud folders with standard access permissions. Sharing limited to internal users.
Confidential	Information that, if accessed by unauthorised individuals, may cause harm to individuals or the company.	• Client proposals • Client Contracts	Access limited to relevant departments (Self Storage)	Must be stored in password-protected folders or locked cabinets. Emailing only with encryption or secure systems. Not to be left unattended.
Restricted	Highly sensitive information requiring strict access control. Unauthorised access could result in legal, reputational, or financial harm.	• ID/Passports documents • Bank details • POPIA compliant Registers	Access strictly limited to designated staff.	Stored in encrypted systems or locked physical safes. Multi-factor authentication (MFA) required for system access. No external sharing without encryption and authorisation.

G. DATA RETENTION AND DESTRUCTION

Eezispace Self Storage Services is committed to retaining personal and business information only for as long as necessary to fulfil the original purpose of collection or as required by applicable legislation, industry standards, or contractual obligations.

Retention periods are carefully assessed based on:

- The nature and sensitivity of the data (e.g., client contracts and documentation)
- Applicable legal and regulatory retention periods (e.g., SARS, BCEA, UIF)
- Operational requirements for self storage.
- Potential future need for audit, dispute resolution, or legal reference

Retention is managed in accordance with the **Eezispace Self Storage Services Data Retention Schedule (Schedule 1)**, which forms part of the broader Information Governance Framework. This schedule outlines prescribed retention periods for specific categories of records and provides employees with clear guidance on data lifecycle expectations.

Secure Storage

The secure storage of data—both digital and physical—is central to Eezispace Self Storage Services' data protection strategy.

- Digital records (e.g., client contracts, Id's and Passports) are stored in secure, access-controlled environments using encrypted servers, firewalls, and multi-factor authentication.
- Physical records (e.g., signed contracts, ID copies, passports) are stored in locked cabinets, with access restricted to authorised personnel.
- All locations—whether at head office, regional offices, or client-based worksites—must implement appropriate security controls to prevent theft, damage, or unauthorised access.

Systems and processes are regularly audited to ensure compliance with internal data security standards and external legal requirements.

Data Destruction

Once data reaches the end of its approved retention period as defined in Schedule 1, Eezispace Self Storage Services ensures that it is permanently and securely destroyed.

Destruction procedures are based on the classification and format of the data:

- **Electronic files** are deleted using certified secure-deletion software that ensures irretrievability.
- **Paper documents** are shredded using cross-cut shredders or disposed of through accredited document destruction services.
- **Portable storage devices** (e.g., USBs or external hard drives) are wiped using industry-grade software or physically destroyed.

All destruction is carried out in a manner that guarantees data cannot be reconstructed, in accordance with POPIA requirements and data protection best practices.

The process is monitored and documented to ensure:

- Irreversibility of data disposal
- Secure handling throughout the destruction chain
- Compliance with internal policies and legal standards

Records Management

To support accountability and regulatory compliance, Eezispace Self Storage Services maintains a full record of all data retention and destruction activities.

These records include:

- The category and format of data retained
- Associated retention periods as per Schedule 1
- The destruction method used
- The date of disposal
- The name of the individual or service provider responsible for the disposal

This transparent recordkeeping framework ensures Eezispace Self Storage Services can demonstrate its compliance during audits, inspections, and internal reviews. It also builds stakeholder trust by showing that data is handled responsibly throughout its lifecycle.

SCHEDULE 1

Record Type	Examples	Retention Period	Legal / Operational Justification	Disposal Method
Employee Records	Contracts, onboarding documents, personal info, disciplinary records	5 years after termination of employment	BCEA, SARS, POPIA	Shredding (physical), Secure digital deletion
Client Contracts	Payslips, earnings, PAYE, UIF, SDL data	5 years	SARS, Income Tax Act	Encrypted digital deletion or shredding
Employee Docs	Employee work hours, shift schedules	3 years	BCEA	Secure disposal, unless part of payroll
Financial Records	Invoices, payments, expense logs	5 years	SARS, Companies Act	Secure digital archive, then deletion
Tax and UIF Submissions	EMP201, EMP501, IRP5s	5 years	SARS, UIF Act	Secure destruction after retention
PAIA & POPIA Documentation	Privacy policies, manuals, consent forms	While active + 5 years post-updates	POPIA, PAIA	Secure digital or paper shredding
Marketing and Communication Consent	Email opt-ins, SMS consents	Until consent withdrawn or service ends	POPIA	Secure deletion upon withdrawal
IT Access Logs and Security Records	System access logs, device usage	1 year	Operational risk management	Secure deletion after review

Notes:

- Retention periods are minimum requirements. Some records may be retained longer if required for active legal proceedings or audits.
- All data disposal must follow Eezispace Self Storage Services' **Data Destruction Policy** to ensure compliance with POPIA's "data no longer required" principle.
- Where retention is based on consent (e.g., self storage), ensure consent documentation is stored with the associated data and reviewed periodically.

H. VENDOR MANAGEMENT

Eezispace Self Storage Services engages with clients with their self storage requirements. When these third parties process personal information on behalf of Eezispace Self Storage Services, they are regarded as "Operators" under POPIA.

Before engaging any operator, Eezispace Self Storage Services must conduct thorough due diligence to assess the operator's data protection capabilities. This includes evaluating their:

- Data privacy policies and POPIA compliance measures
- Security infrastructure (e.g. encryption, access controls, breach response protocols)
- History of compliance with applicable data protection legislation
- Capacity to maintain the confidentiality and integrity of personal information

All operator relationships must be governed by written agreements that clearly outline:

- The specific personal information to be processed
- The operator's duties in relation to security, confidentiality, and lawful processing
- Breach notification requirements
- Restrictions on data transfer, use, or further disclosure without approval
- Terms for secure data return or destruction at the end of the engagement

Eezispace Self Storage Services remains ultimately accountable for the processing of personal information, even when carried out by an operator.

I. BREACH MANAGEMENT

Reporting and Investigation

All employees, contractors, and service providers must immediately report any actual or suspected data breach to the Information Officer or designated authority. Prompt reporting is critical to protect affected data subjects and contain the risk.

An Incident Response Plan shall be activated upon notification of a breach. This includes:

- A rapid investigation into the scope and cause

- Risk assessment and categorisation
- Immediate containment and recovery actions
- Documentation of the incident and mitigation steps

Notification and Communication

If a breach is likely to result in harm to a data subject (e.g. identity theft, financial loss, or reputational damage), Eezispace Self Storage Services will notify:

- The affected individual(s), as required under POPIA
- The Information Regulator of South Africa
-

All notifications must include sufficient detail of the breach, potential consequences, and actions the data subject can take to protect themselves. Notification will be done as soon as reasonably possible, in plain and accessible language.

J. POLICY COMPLIANCE AND REVIEW

Eezispace Self Storage Services is committed to ensuring continuous alignment with this policy through regular compliance monitoring and internal audits. These assessments ensure that all departments uphold the data protection responsibilities defined in this policy.

The policy will be reviewed annually, or sooner if there are:

- Changes to data protection legislation
- New or evolving risks in data processing activities
- Operational changes affecting the scope or implementation of compliance practices

All revisions must be communicated to employees, who will be required to acknowledge their understanding and commitment to the updated policy.

K. POLICY BREACH

This policy is binding on all employees, contractors, operators, and any third party acting on behalf of Eezispace Self Storage Services.

Failure to comply with this policy—whether through negligence, misconduct, or deliberate disregard—constitutes a policy breach and will be treated seriously. This includes non-compliance with access control measures, unauthorised data disclosure, or failure to report a known breach.

L. ENFORCEMENT

Employees found in violation of this policy may be subject to internal disciplinary procedures, up to and including termination of employment.

Contractors, vendors, or operators in breach of this policy may have their contracts terminated, and may be reported to relevant regulators if non-compliance poses legal or reputational risk to Eezispace Self Storage Services.

Any exception to the policy must be formally documented and approved in accordance with the Exception Management Procedure.

POLICY AMENDMENTS

Date	Page	Amendment	Signature

POLICY APPROVED BY

Name	Date	Signature