

**POLICY STATEMENT AND MANUAL OF:**  
**PROTECTION OF PERSONAL INFORMATION  
AND THE RETENTION OF DOCUMENTATION**

for

**REGENESYS MANAGEMENT (PTY) LIMITED**

and its subsidiaries

(Hereinafter referred to as "Regenesys")

Registration Number: 1997/009003/07

This policy is drafted in compliance with, and in response to, the Protection of Personal Information Act, 4 of 2013 and the Regulations to the Act (hereinafter referred to as "POPI")

This policy aims to uphold, promote and protect the underpinning principles of the POPI Act



# PROTECTION OF PERSONAL INFORMATION



## **PART A**

### **1.1. INTRODUCTION**

Regenesys is a private company duly incorporated in accordance with the laws of the Republic of South Africa. Regenesys is a registered Higher Education Institution and carries on business by providing educational learning programmes and with its principal place of business at 165 West Street, Sandown, Sandton, 2031.

Regenesys Management (Pty) Ltd and its subsidiaries are a group of companies functioning within the private higher education sector within the territory of the Republic of South Africa and is obligated to comply with the Protection of Personal Information Act, 4 of 2013 ("POPI).

POPI requires the Regenesys group of companies to inform their clients as to the manner in which their personal information is collected, used, stored, disclosed and subsequently destroyed.

Regenesys guarantees its commitment to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The policy sets out the manner in which Regenesys deals with their client's personal information and stipulates the purpose for which the said information is used. This policy is made available on the Regenesys Website and upon request from the Regenesys Legal & Compliance Department.

### **1.2. COLLECTION OF PERSONAL INFORMATION**

For the purposes of this policy, clients refers to both potential and existing clients.

Regenesys undertakes to only collect and process client's personal information pertaining to the client's educational or financial needs. The nature of the information required depends on the nature of client's needs and the purpose and requirements for which the information must be collected. Wherever possible, Regenesys will inform the client of the information required, information that is optional and the reasons for same.

**Examples of personal information that Regenesys may collect in order to render services to its clients include, but is not limited to:**

- Client's identity/passport numbers
- Client's names, surnames, addresses and proof thereof (as per FICA requirements), postal codes, marital status and number of dependents
- Description of client's places of residence, businesses, assets, bank statements and/or financial information, proof of banking details etc.
- Any other relevant information required by Regenesys in order to render services to the client as may be required and/or permissible in law.

Regenesys also lawfully collects and processes their client's personal information for marketing purposes subject to the client's knowledge and consent in order to ensure that our services and products remain relevant to our clients and to potential clients.

Regenesys aims to have agreements in place with all product suppliers, insurers and third-party service providers to ensure a mutual understanding with regard to the protection of the client's personal information. Regenesys undertakes to make use of service providers and third parties who are committed to upholding the underpinning values of POPI and data protection. No confidential information is shared with third parties or service providers without the client's prior consent.

## 1.3. USE OF PERSONAL INFORMATION

Client's personal information will only be used for the purpose and to the extent that it is necessary and relevant for Regenesys to supply services and goods to the client.

**This may include, but is not limited to:**

- Providing products or services to clients and to carry out the transactions requested
- For providing accredited educational programmes
- For assessment and reporting purposes insofar as accreditation may be required
- For underwriting purposes
- Assessing and processing claims
- Conducting credit reference searches or verification
- Confirming, verifying, and updating client details
- For the purposes of verifying client history
- To prevent crime, fraud, money laundering or any other malpractices
- To comply with any law, statute, or regulation
- To conduct audits and for recordkeeping purposes
- In connection with legal proceedings
- Providing services to clients, rendering services requested by clients and maintaining client relationships

**The aforementioned categories of personal information are processed inter alia in accordance with section 10 of POPI. Such personal information may only be processed if certain conditions, listed below are met and accompanied by supporting documentation:**

- The client's full and informed consent is obtained; and
- The information to be processed is necessary, adequate, and relevant and is causally linked to the purpose for which it is being collected.
- The collection of such information must not be excessive.
- Processing of personal information complies with an obligation imposed by law on the Regenesys group.
- The processing protects a client's legitimate interest, and it is in the client's best interests to disclose the personal information
- Processing is necessary for pursuing the legitimate interests of the Regenesys group or a third-party/supplier whose services clients elect to use.

The Regenesys group assures that it has agreements in place with its employees, contractors, suppliers and third parties to whom personal information is supplied to uphold data protection and privacy.

## 1.4. DISCLOSURE OF PERSONAL INFORMATION

Regenesys Management (Pty) Ltd may disclose a client's personal information to any of the Regenesys subsidiaries and or approved/verified product or third-party service providers whose services or products clients elect and consent to use or use as a consequence of their agreement with the Regenesys group.

Confidentiality and data protection agreements are in place to adequately protect personal information and uphold the privacy of the data subject.

Regenesys may also share client personal information with and obtain information for third parties or service providers for reasons mentioned above.

Regenesys may also disclose a client's information where it has a duty or a right to disclose same in terms of any applicable legislation, regulation or where it is deemed necessary to protect Regenesys' rights.

## 1.5. SAFEGUARDING OF CLIENT INFORMATION

It is a requirement of POPI to adequately protect personal information. Regenesys commits to continuously reviewing its security measures and processes to ensure that personal information is kept secure.

**The following procedures are in place in order to protect personal information:**

- 1.5.1. The policy has been put in place throughout the Regenesys group and training on this policy and the POPI Act will be implemented and put in place for all staff contractors and/or any other interested or relevant parties;
- 1.5.2. Every employee in the Regenesys group will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the POPI Act;
- 1.5.3. Every employee currently employed within the Regenesys group will be required to sign an addendum to their employment contracts containing the relevant clauses for the use, storage and protection of any relevant data subject's personal information including, but not limited to, suppliers, clients and third parties;
- 1.5.4. Archived information is stored securely on site in accordance with POPI with limited access to authorised personnel only;
- 1.5.5. Any personal information in hard-copy form is kept for the time required by law and destroyed thereafter through the use of appropriate equipment;
- 1.5.6. Regenesys suppliers, insurers and third-party service providers will be required to sign service level agreements guaranteeing their commitment and compliance with POPI;
- 1.5.7. All electronic files and data are securely backed up and stored on internal and third-party servers that have the requisite security measures in place to prevent data breaches and physical threats.

Consent to process client's information is obtained from clients (or such a person who is duly authorised to act on the client's behalf) during the commencement of any relationship.

## 1.6. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

Clients have the right to access their personal information as data subjects insofar as it is being held by the Regenesys group. Clients have the right to request that their personal information be updated, changed, corrected and/or deleted on reasonable grounds subject to verification and necessary approval. Should a client object to the processing of their personal information or making changes to their personal information, the Regenesys group shall no longer process said personal information. Regenesys takes all reasonable steps to confirm its clients' identities before providing any details of their personal information or making changes to their personal information.

### **HEAD OFFICE DETAILS:**

**PHYSICAL ADDRESS:** 165 West Street, Sandown, Sandton, 2196

**POSTAL ADDRESS:** Postnet Suite 71, Private Bag X9976, Sandton City, 2146, South Africa

**TELEPHONE NUMBER:** (011) 669 5000

**FAX NUMBER:** (011) 669 5001

**EMAIL ADDRESS:** [info@regenesys.net](mailto:info@regenesys.net)

**WEBSITE:** [www.regenesys.net](http://www.regenesys.net)

## 2. AMENDMENTS TO POLICY

Any amendments to, or reviewing of, this policy shall take place on an ad hoc basis or on an annual basis. Clients are always advised to access Regenesys' website periodically to stay informed of any changes to our policies. Should any material changes be effected, Regenesys shall inform affected parties.

## 3. RECORDS THAT CANNOT BE FOUND

Should any records held by Regenesys for whatsoever reason or cause arising go missing or are destroyed (including but not limited to force majeure events), the data subject will be notified by way of a sworn affidavit. The affidavit deposited to by a duly authorised representative of Regenesys shall make reference to how the records were lost, misplaced and/or destroyed.

---

## PART B

### POLICY ON THE RETENTION AND CONFIDENTIALITY OF DOCUMENTS, PERSONAL INFORMATION AND ELECTRONIC TRANSACTIONS

#### 1. PURPOSE

- 1.1. To exercise effective control over the retention of documents and electronic transactions as prescribed by law and as dictated by business practice.
- 1.2. Documents need to be retained in order to prove the existence of facts and to exercise rights the Company may have. Documents are also necessary with regards to any litigation which may subsequently arise to protect Regenesys' rights in law.
- 1.3. To ensure that the Company's rights in law remain protected and that the Company and its client's privacy and confidentiality is not breached.
- 1.4. To ensure that the Company's interests are protected and that the Company's and client's rights to privacy and confidentiality are not breached.
- 1.5. Queries may be referred to the Head Office.

#### 2. SCOPE AND DEFINITIONS

- 2.1. All documents and electronic transactions generated within and/or received by the Company.

##### Definitions

- 2.2. "Clients" includes, but is not limited to, shareholders, debtors, students, creditors as well as any affected personnel and/or departments related to a service division of the Company.
- 2.3. "Confidential Information" refers to all information or data disclosed to, or obtained by, the Company through any means whatsoever and shall include, but not be limited to:
  - 2.3.1. financial information and records;
  - 2.3.2. all other information, including information relating to the structure, operations, processes, intentions, product information, know-how, trade secrets, market opportunities, customers and business affairs subject to where lawful disclosure is required.

- 2.3.3. "Constitution" refers to the Constitution of the Republic of South Africa, 108 of 1996.
- 2.3.4. "Data" refers to electronic representations of information in any form.
- 2.3.5. "Documents" includes books, records, security or account and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.
- 2.3.6. "ECTA" refers to the Electronic Communications and Transactions Act, 25 of 2002.
- 2.3.7. "Electronic communication" refers to communication by means of data messages.
- 2.3.8. "Electronic signature" refers to data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature.
- 2.3.9. "Electronic transactions" refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.
- 2.3.10. "Electronic transactions" includes electronic mails sent and received.
- 2.3.11. "PAIA" refers to Promotion of Access to Information Act, 2 of 2002.

## 3. CONTENTS

- 3.1. See Annexure "A" attached hereto (available on request).

## 4. ACCESS TO DOCUMENTS

- 4.1. **All Company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear or redress, in the following circumstances (see clause 4.2 below):**
  - 4.1.1. where disclosure is under compulsion of law;
  - 4.1.2. where there is a duty to the public to disclose any information in the public interest;
  - 4.1.3. where there is an interest to disclose on behalf of the company; and
  - 4.1.4. where disclosure is made with the express or implied consent of the data subject.
- 4.2. **DISCLOSURE TO 3RD PARTIES:**  
**All employees have a duty of confidentiality in relation to the company and clients. In addition to the provisions of clause 4.1 above, the following are also applicable:**
  - 4.2.1. We acknowledge our client's right to confidentiality and privacy as contained in the provisions of the Constitution and the ECTA. Clients may consent in writing to have their personal information shared with third parties.
  - 4.2.2. Requests for information are dealt with in accordance with the governing provisions of PAIA, however, the Company may refuse access to such information for any lawful reasons whatsoever, including compliance with the provisions of POPI.
  - 4.2.3. Parties requesting such information are required to do so in writing, stating their reasons therefore, and may undertake to pay any such fees as may be applicable to retrieve and access same.
  - 4.2.4. Confidential company and/or business information may not be disclosed to third parties as this could constitute a breach of intellectual property rights and allude to corporate espionage. The affairs of the company are to be kept confidential at all times.
- 4.3. The company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary proceedings.

## 5. STORAGE OF DOCUMENTS

### HARD COPIES

- 5.1. Hard copies are stored on secure archiving premises with limited authorised access to authorised personnel only.
- 5.2. All hard copies are kept for 7 years in accordance with the provisions of the Companies Amendment Act, 3 of 2011 or for any other time period as specified and stipulated by law, including, but not limited to, the National Credit Act, 34 of 2005; the Consumer Protection Act, 68 of 2008; the Financial Advisory and Intermediary Services Act, 37 of 2002; the Financial Intelligence Centre Act, 38 of 2001; the Compensation for Occupational Injuries and Diseases Act, 130 of 1993; Basic Conditions of Employment Act, 75 of 1997; Employment Equity Act, 55 of 1998; Labour Relations Act, 66 of 1995; Unemployment Insurance Act, 63 of 2002; Tax Administration Act, 28 of 2011; Income Tax Act, 58 of 1962; Value Added Tax Act, 89 of 1991.
- 5.3. Any other documents required by law to be retained indefinitely are stored accordingly.

## 6. ELECTRONIC STORAGE

- 6.1. The internal procedure requires that electronic storage of information is overseen by the IT department and CIO who arrange for the secure storage, indexing and retrieval thereof.
- 6.2. **Scanned documents:** If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.
- 6.3. Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used.
- 6.4. It is also required that all personal information which has become obsolete must be destroyed.

## 7. DESTRUCTION OF DOCUMENTS

- 7.1. Documents may be destroyed after the termination of the retention period specified in Annexure "A" hereto. Registration will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.
- 7.2. Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.
- 7.3. After completion of the process in 6.2 above, the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by Registration.
- 7.4. The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.
- 7.5. Documents may also be stored off-site, in storage facilities approved by the Company.