POPI Policy

Policy statement and manual of Protection of Personal, Information and the Retention of Documents for Monitor Net CC and all its subsidiaries (hereinafter referred to as "Monitor Net") (Registration number: **1994/39115/23**)

Index

Protection of personal information in terms of the Protection of Personal Information Act 4 of 2013

1. Protection of Personal Information Act, 4 Of 2013

1.1. Introduction

Monitor Net is a company functioning within the security sector, that is obligated to comply with The Protection of Personal Information Act 4 of 2013. POPI requires Monitor Net to inform their clients as to the manner in which their personal information is used, disclosed and destroyed.

Monitor Net is committed 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 Monitor Net deals with their client's personal information as well as stipulates the purpose for which said information is used. The Policy is made available on Monitor Net company website www.monitornet.co.za and by request from Monitor Net head office.

1.2. Personal Information Collected

Section 9 of POPI states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

Monitor Net collects and processes client's personal information pertaining to the client's security needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, Monitor Net will inform the client as to the information required and the information deemed optional. Examples of personal information we collect include, but is not limited to:

1.2.1. The Client's Identity number, name, surname, address, postal code, marital status, and number of dependants;

1.2.2. Description of the client's residence, financial information, banking details, etc-.

1.2.3. Any other information required by Monitor Net or suppliers in order to provide clients with an accurate service delivery needs.

Monitor Net also collects and processes the client's personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

Monitor Net aims to have agreements in place with all product suppliers and third party service providers to ensure a mutual understanding with regard to the protection of the client's personal information. Monitor Net suppliers will be subject to the same regulations as applicable to Monitor Net.

With the client's consent, Monitor Net may also supplement the information provided with information Monitor Net receives from other providers in order to offer a more consistent and personalized experience in the client's interaction with Monitor Net. For purposes of this Policy, clients include potential and existing clients.

1.3. The Usage Of Personal Information

The Client's Personal Information will only be used for the purpose for which it was collected and as agreed. This may include:

1.3.1. Providing products or services to clients and to carry out the transactions requested;

1.3.2. For underwriting purposes;

1.3.3. Assessing and processing claims;

1.3.4. Confirming, verifying and updating client details;

1.3.5. For purposes of call out history;

1.3.6. For the detection and prevention of fraud, crime, money laundering or other malpractices;

1.3.7. Conducting market or customer satisfaction research;

1.3.8. For audit and record keeping purposes;

1.3.9. In connection with legal proceedings;

1.3.10. Providing Monitor Net services to clients, to render the services requested and to maintain and constantly improve the relationship;

1.3.11. Providing communication in respect of Monitor Net and regulatory matters that may affect clients; and

1.3.12. In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

1.3.13. According to section 10 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for Monitor Net processing of Personal Information:

- The client's consents to the processing: - consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;
- The necessity of processing: in order to conduct an accurate analysis of the client's needs for purposes of amongst other credit limits, insurance requirements, etcetera.
- Processing complies with an obligation imposed by law on Monitor Net;
- Processing protects a legitimate interest of the client — it is in the client's best interest to have a full and proper needs analysis performed in order to provide them with an applicable and beneficial product or service.
- Processing is necessary for pursuing the legitimate interests of Monitor Net or of a third party to whom information is supplied — in order to provide Monitor Net clients with products and or services both Monitor Net and any of our product suppliers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.

1.4. Disclosure Of Personal Information

1.4.1. Monitor Net may disclose a client's personal information to any of the Monitor Net subsidiaries, joint venture companies and or approved product supplier or third party service providers whose services or products clients elect to use. Monitor Net has agreements in place to ensure compliance with confidentiality and privacy conditions.

1.4.2. Monitor Net may also share client personal information with, and obtain information about clients from third parties for the reasons already discussed above.

1.4.3. Monitor Net may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect Monitor Net rights.

1.5. Safeguarding Client Information

1.5.1. It is a requirement of POPI to adequately protect personal information. Monitor Net will continuously review its security controls and processes to ensure that personal information is secure.

1.6.1. The Monitor Net Information Officer is Wynand Grove whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI. Wynand Grove is assisted by Paul Gerber who will function as the Group's Deputy Information Officer;

1.6.2. This policy has been put in place throughout Monitor Net and training on this policy and the POPI Act has already taken place and will be conducted during 2019 by Monitor Net.

1.6.3. Each new employee will be required to sign an EMPLOYMENT CONTRACT containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI;

1.6.4. Every employee currently employed within Monitor Net 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 POPI;

1.6.5. Monitor Net archived client information is stored off site at Metrofile which is also governed by POPI, access to retrieve information is limited to authorized personal.

1.6.6. Monitor Net product suppliers, insurers and other third party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

1.6.7. All electronic files or data are backed up by Monitor Net's IT Division which is also responsible for system security that protects third party access and physical threats. The IT Division is responsible for Electronic Information Security;

1.7. Access And Correction Of Personal Information

Clients have the right to access the personal information Monitor Net holds about them. Clients also have the right to ask Monitor Net to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, Monitor Net may no longer process said personal information. Monitor Net will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

The details of Monitor Net's Information Officer and Head Office are as follows:

Information Officer	Wynand Grove
Telephone Number	0861 117 117
Fax Number	N/A
E-Mail Address	wgro@monitornet.co.za
Deputy Information Officer	Paul Gerber

Telephone Number	0861 117 117
Fax Number	N/A
E-Mail Address	ops@monitornet.co.za

Head Office Details	
Telephone	0861 117 117
Fax	086 680 8536
Postal	P.O Box 16257 ,Lyttelton,0140
Physical	690 Tobie str Hennopspark

2. Amendments to this policy

Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year. Clients are advised to access Monitor Net's website periodically to keep abreast of any changes. Where material changes take place, clients will be notified directly or changes will be stipulated on the Monitor Net website.

Policy on the retention & confidentiality of documents, information and electronic transactions

1. Purpose

1.1. To exercise effective control over the retention of documents and electronic transactions:

1.1.1. as prescribed by legislation; and

1.1.2. 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 for defending legal action, for establishing what was said or done in relation to business of the Company and to minimize the Company's reputational risks.

1.3. To ensure that the Company's interests are protected and that the Company's and clients' rights to privacy and confidentiality are not breached.

1.4. Queries may be referred to the Company Secretary.

2. Scope and Definitions

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

2.2. Definitions:

2.2.1. Clients includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.

2.2.2. Confidential Information refers to all information or data disclosed to or obtained by the Company by any means whatsoever.

2.2.3. Constitution: Constitution of the Republic of South Africa Act, 108 of 1996.

2.2.4. Data refers to electronic representations of information in any form.

2.2.5. Documents include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

2.2.6. ECTA: Electronic Communications and Transactions Act, 25 of 2002.

2.2.7. Electronic communication refers to a communication by means of data messages.

2.2.8. 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.

2.2.9. Electronic transactions include e-mails sent and received.

2.2.10. PAIA: Promotion of Access to Information Act, 2 of 2000.

3. Access to Documents

3.1. All Company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 4.2 below):

3.1.1. where disclosure is under compulsion of law;

3.1.2. where there is a duty to the public to disclose;

3.1.3. where the interests of the Company require disclosure; and

3.1.4. where disclosure is made with the express or implied consent of the client.

4. Disclosure to 3rd Parties

4.1. All employees have a duty of confidentiality in relation to the Company and clients.

4.1.1. Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the client has consented in writing to that person receiving the information.

4.1.2. Requests for company information:

- These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.
- In terms hereof, requests must be made in writing on the prescribed form to the Company Secretary, who is also the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.
- The Company's manual in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is available on the intranet and the Monitor Net website www.monitornet.co.za .

4.1.3. Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be kept strictly confidential at all times.

4.2. The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

5. Storage of Documents

5.1. Hard Copies

5.1.1. Documents are stored in an archive different location.

5.1.2. Companies Act, No 71 of 2008:

- With regard to the Companies Act, No 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for 7 years:
  - Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;
  - Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities;
  - Copies of reports presented at the annual general meeting of the company;
  - Copies of annual financial statements required by the Act;
  - Copies of accounting records as required by the Act;
  - Record of directors and past directors, after the director has retired from the company;
  - Written communication to holders of securities and
  - Minutes and resolutions of directors' meetings, audit committee and directors' Committees
- Copies of the documents mentioned below must be retained indefinitely:
  - Registration certificate;
  - Memorandum of Incorporation and alterations and amendments;
  - Rules;
  - Securities register and uncertified securities register;
  - Register of company secretary and auditors and
  - Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

5.1.3. Consumer Protection Act, No 68 of 2008:

- The Consumer Protection Act seeks to promote a fair, accessible and sustainable market place and therefore requires a retention period of 3 years for information provided to a consumer by an intermediary such as:
  - Full names, physical address, postal address and contact details;
  - ID number and registration number;
  - Contact details of public officer in case of a juristic person;

- Service rendered;
- Intermediary fee;
- Cost to be recovered from the consumer;
- Frequency of accounting to the consumer;
- Amounts, sums, values, charges, fees, remuneration specified in monetary terms;
- Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided;
- Record of advice furnished to the consumer reflecting the basis on which the advice was given;
- Written instruction sent by the intermediary to the consumer;
- Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;
- Documents Section 45 and Regulation 31 for Auctions.

5.1.4. Financial Intelligence Centre Act, No 38 of 2001:

− Section 22 and 23 of the Act require a retention period of 5 years for the documents and records of the activities mentioned below:

- Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client;
- If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the clients authority to act on behalf of that other person;
- If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client;
- The manner in which the identity of the persons referred to above was established;
- The nature of that business relationship or transaction;
- In the case of a transaction, the amount involved and the parties to that transaction;
- All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction;
- The name of the person who obtained the identity of the person transacting on behalf of the accountable institution;
- Any document or copy of a document obtained by the accountable institution.
- These documents may also be kept in electronic format.

5.1.5. Compensation for Occupational Injuries and Diseases Act, No 130 of 1993:

− Section 81(1) and (2) of the Compensation for Occupational Injuries and Diseases Act requires a retention period of 4 years for the documents mentioned below:

- Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.

- Section 20(2) documents with a required retention period of 3 years:
  - Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;
  - Records of incidents reported at work.
  - Asbestos Regulations, 2001, regulation 16(1) requires a retention period of minimum 40 years for the documents mentioned below:
    - Records of assessment and air monitoring, and the asbestos inventory;
    - Medical surveillance records;
    - Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):
    - Records of risk assessments and air monitoring; − Medical surveillance records.
- Lead Regulations, 2001, Regulation 10:
  - Records of assessments and air monitoring; • Medical surveillance records.
- Noise - induced Hearing Loss Regulations, 2003, Regulation 11:
  - All records of assessment and noise monitoring;
  - All medical surveillance records, including the baseline audiogram of every employee. Hazardous Chemical Substance Regulations, 1995, Regulation 9 requires a retention period of 30 years for the documents mentioned below:
    - Records of assessments and air monitoring; − Medical surveillance records.

5.1.6. Basic Conditions of Employment Act, No 75 of 1997:

- The Basic Conditions of Employment Act requires a retention period of 3 years for the documents mentioned below:
  - Section 29(4):
    - Written particulars of an employee after termination of employment;
  - Section 31:
    - Employee's name and occupation;
    - Time worked by each employee;
    - Remuneration paid to each employee;
    - Date of birth of any employee under the age of 18 years.

5.1.7. Employment Equity Act, No 55 of 1998:

- Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 3 years for the documents mentioned below:
  - Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;
- Section 21 and Regulations 4(10) and (11) require a retention period of 3 years for the report which is sent to the Director General as indicated in the Act.

5.1.8. Labour Relations Act, No 66 of 1995:

- Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:

  - The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
  - Registered Trade Unions and registered employer's organizations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
  - Registered Trade Unions and employer's organizations must retain the ballot papers;
  - Records to be retained by the employer are the collective agreements and arbitration awards.

− Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents mentioned below:

  - Registered Trade Unions and registered employer's organizations must retain a list of its members;
  - An employer must retain prescribed details of any strike action involving its employees;
  - Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions;
  - The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.

5.1.10. Unemployment Insurance Act, No 63 of 2002:

− The Unemployment Insurance Act, applies to all employees and employers except:

  - Workers working less than 24 hours per month;
  - Learners;
  - Public servants;
  - Foreigners working on a contract basis;
  - Workers who get a monthly State (old age) pension;
  - Workers who only earn commission.

− Section 56(2)(c) requires a retention period of 5 years, from the date of submission, for the documents mentioned below:

  - Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.

5.1.11. Tax Administration Act, No 28 of 2011:

− Section 29 of the Tax Administration Act, states that records of documents must be retained to:

  - Enable a person to observe the requirements of the Act;
  - Are specifically required under a Tax Act by the Commissioner by the public notice;

- Will enable SARS to be satisfied that the person has observed these requirements.

− Section 29(3)(a) requires a retention period of 5 years, from the date of submission for taxpayers that have submitted a return and an indefinite retention period, until the return is submitted, then a 5 year period applies for taxpayers who were meant to submit a return.

− Section 29(3)(b) requires a retention period of 5 years from the end of the relevant tax period for taxpayers who were not required to submit a return, but had capital gains/losses or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.

− Section 32(a) and (b) require a retention period of 5 years but records must be retained until the audit is concluded or the assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.

5.1.12. Income Tax Act, No 58 of 1962:

− Schedule 4, paragraph 14(1)(a)-(d) of the Income Tax Act requires a retention period of 5 years from the date of submission for documents pertaining to each employee that the employer shall keep:

- Amount of remuneration paid or due by him to the employee;
- The amount of employees tax deducted or withheld from the remuneration paid or due;
- The income tax reference number of that employee;
- Any further prescribed information;
- Employer Reconciliation return.

− Schedule 6, paragraph 14(a)-(d) requires a retention period of 5 years from the date of submission or 5 years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to:

- Amounts received by that registered micro business during a year of assessment;
- Dividends declared by that registered micro business during a year of assessment;
- Each asset as at the end of a year of assessment with cost price of more than R 10 000;
- Each liability as at the end of a year of assessment that exceeded R 10 000.

5.1.13. Value Added Tax Act, No 89 of 1991:

− Section 15(9), 16(2) and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, 30 March requires a retention period of 5 years from the date of submission of the return for the documents mentioned below:

- Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;
- Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;

- Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques;
- Documentary proof substantiating the zero rating of supplies;
- Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.

5.2. Electronic Storage

5.2.1. The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

5.2.2. 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.

5.2.3. 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. It is also required that all personal information which has become obsolete must be destroyed.

6. Destruction of Documents

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

6.5. Documents may also be stored off-site, in storage facilities approved by the Company.