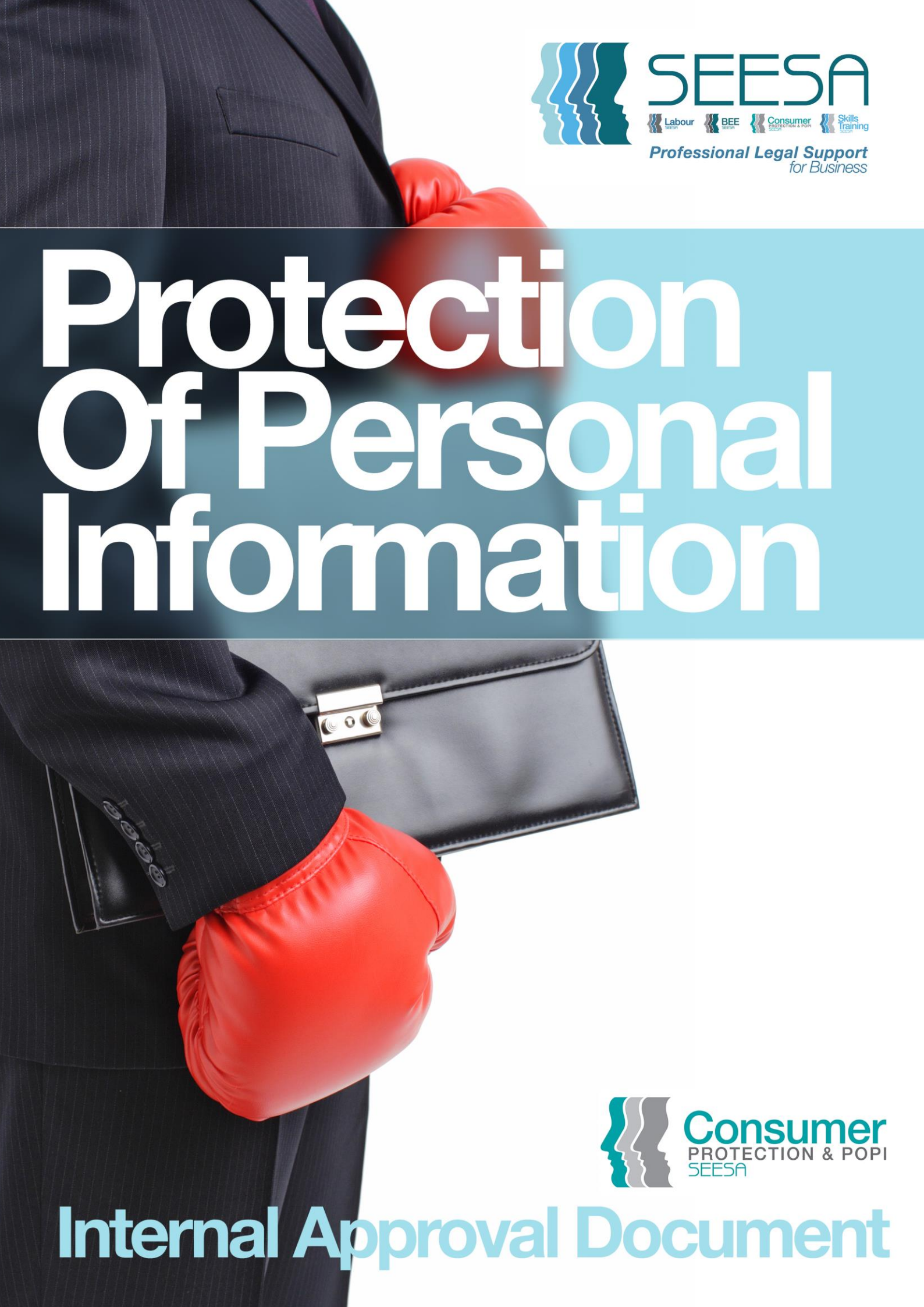

SEESA

Labour BEE Consumer PROTECTION & POPI Skills Training

Professional Legal Support for Business

Protection Of Personal Information

Consumer PROTECTION & POPI SEESA

Internal Approval Document

Table of Contents

Internal Approval Document

Approval

Approved on behalf of Prideshelf 1058 CC t/ Rotocon

Name

Designation

Signature

Date

Document Version Control

VERSION	DATE	SUMMARY OF CHANGES
V000		
V001		
V002		
V003		
V004		
V005		
V006		
V007		
V008		
V009		
V010		
V011		
V012		
V013		
V014		
V015		
V016		
V017		

General Processing of Personal Information

Policy	**General Processing of Personal Information**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Preamble

Rotocon is an organisation that complies with the laws of South Africa and recognises that a person's constitutional right to privacy is of the upmost importance, therefore the protection of personal information is vital for **sustainability and growth** of our business.

2. Purpose

The purpose of this policy is to incorporate the requirements of the Protection of Personal Information Act No.4 of 2013 (hereafter called this Act) into the everyday operations of Rotocon and to ensure that these requirements are documented and implemented in Rotocon.

3. Scope

This policy is applicable to all employees in Rotocon.

4. Objectives

Rotocon and its employees shall adhere to this policy in the handling of all personal information received from, but not limited to natural persons, employees, clients, suppliers, agents, representatives and business partners to ensure compliance with this Act, applicable regulations and other rules relating to the protection of personal information.

5. Management Declaration

Rotocon, represented by the Information Officer confirms that we have familiarized ourselves with the content of this Act, applicable regulations and other rules relating to the protection of personal information, and will strive to adhere to these requirements at all times.

6. Important Definitions

"automatic calling machine": means a machine that is able to do automated calls without human intervention;

"binding corporate rules": means personal information processing policies, within a group of undertakings, which are adhered to by Rotocon or operation within that group of undertakings when transferring personal information to a business or operator within that same group of undertakings in a foreign country;

"data subject": means the person to whom personal information relates;

"direct marketing": means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a) Promoting or offering to supply, in the ordinary course of business, any goods or service to the data subject; or

b) Requesting the data subject to make a donation of any kind for any reason.

"electronic communication": means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

"filing system": means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

"group undertakings": means a controlling undertaking and its controlled undertakings;

"information officer": of, or in relation to, a –

a) Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of this Act; or

b) Private body means the head of a private body as contemplated in Section 1 of the Promotion of Access to Information Act.

"operator": means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"person": means a natural person or a juristic person.

"personal information": means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

b) Information relating to the education or the medical, financial, criminal or employment history of the person;

c) Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person;

d) The biometric information of the person;

e) The personal opinions, views or preferences of the person;

f) Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature;

g) The views or opinions of another individual about the person; and

h) The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

"private body": means –

a) A natural person who carries or has carried on any business or profession, but only in such capacity;

b) A partnership which carries or has carried on any trade, business or profession; or

c) Any former or existing juristic person, but excludes a public body.

"processing": means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

b) Dissemination by means of transmission, distribution or making available in any other form; or

c) Merging, linking, as well as restriction, degradation, erasure or destruction of information.

"Promotion of Access to Information Act": means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

"public body": means –

a) Any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

b) Any other functionary or institution when –

I. Exercising a power or performing a duty in terms of the Constitution or provincial constitution; or

II. Exercising a public power or performing a public function in terms of any legislation.

"public record": means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

"record": means any recorded information –

a) Regardless of form or medium, including any of the following:

I. Writing on any material;

II. Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

IV. Book, map, plan, graph, or drawing;

V. Photograph, film, negative, tape or other device in which one or more visuals images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

b) In the possession or under the control of a responsible party; and

c) Regardless of when it came into existence.

"regulator": – means the Information Regulator established in terms of Section 39.

"re-identify": in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that –

a) Identifies the data subject;

b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject, and **'re-identified"** has a corresponding meaning.

"responsible party": means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

"restriction": means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"special personal information": means personal information as referred to in Section 26 of this Act.

"this Act": means the Protection of Personal Information Act, No. 4 of 2013.

"unique identifier": means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

7. Rotocon's key principles in adhering to the requirements of the protection of personal information

Rotocon's and its employees are committed to the following principles:

- To give effect to the constitutional right to privacy, by safeguarding personal information when processed by Rotocon, subject to justifiable limitations;
- To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;
- To be transparent in its standard operating procedures that govern the processing of personal information;
- To comply with the applicable legal and regulatory requirements regarding the processing of personal information;
- To collect personal information through lawful and fair means and to process personal information in a manner compatible with the purpose for which it was collected;
- Where required by law and according to local requirements, to inform data subjects when personal information is collected about them;
- Where required by law, regulations or guidelines, to obtain a data subject's consent prior to processing his/her/its personal information;
- To strive to keep personal information accurate, complete, up-to-date and reliable for its intended use;
- To strive to develop reasonable security safeguards against risks, losses, unauthorised access, destruction, use, modification or disclosure of personal information;
- To strive to provide data subjects with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or rectify the personal information where incomplete, inaccurate or not compliant with the standard operating procedures;

- To only share personal information, such as permitting access, transmission or publication, with third parties (either within or outside Rotocon), only if reasonable assurance can be provided that the recipient of such information will apply suitable privacy and security protection to the personal information;
- To comply with any restrictions and requirements that applies to the Transborder Information Flow Policy.

8. Procurement of Personal Information

8.1 Personal information collected by Rotocon and/or any of its representatives, will be collected directly from the data subject, unless –

a) The information is contained or derived from a public record or has deliberately been made public by the data subject;

b) The data subject or a competent person where the data subject is a child, has consented to the collection of the information from another source;

c) Collection of the information from another source would not prejudice a legitimate interest of the data subject;

d) Collection of the information from another source is necessary –

I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

IV. In the interest of national security; or

V. To maintain the legitimate interests of Rotocon or of a third party to whom the information is supplied;

e) Compliance would prejudice a lawful purpose of the collection; or

f) Compliance is not reasonably practicable in the circumstances of the particular case.

8.2 Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of Rotocon.

8.3 Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.

8.4 Rotocon will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected and further processed.

8.5 Where personal information is collected form a data subject, Rotocon will take reasonably practicable steps to ensure that the data subject is aware of –

a) The information being collected and where the information is not collected from the data subject, the source from which it is collected;

b) The name and address of Rotocon;

c) The purpose for which the information is being collected;

d) Whether or not the supply of the information by the data subject is voluntary or mandatory;

e) The consequences of failure to provide the information;

f) Any particular law authorising or requiring the collection of the information;

g) The fact that, where applicable, Rotocon intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisations;

h) Any further information such as the –

I. Recipient or category of recipients of the information;

II. Nature or category of the information;

III. Existence of the right of access to and the right to rectify the information collected;

IV. Existence of the right to object to the processing of personal information ;

Which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

8.6 The steps referred to in clause 8.5 must be taken –

a) If the personal information is collected directly from the data subject, prior to the information being collected, unless the data subject is already aware of the information as referred to in clause 8.5;

b) In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

8.7 It will not be necessary for Rotocon to comply with clause 8.5 if –

a) The data subject or a competent person if the data subject is a child has provided consent for the non-compliance;

b) Non-compliance would not prejudice the legitimate interests of the data subject;

c) Non-compliance is necessary –

I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

IV. In the interest of national security.

d) Compliance would prejudice a lawful purpose of the collection;

e) Compliance is not reasonably practicable in the circumstances of the particular case; or

f) The information will –

I. Not be used in a form in which the data subject may be identified; or

II. Be used for historical, statistical or research purposes.

9. Processing of Personal Information

9.1 Personal information will only be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

9.2 Personal information may only be processed if –

a) given the purpose for which it was processed, it is adequate, relevant and not excessive;

b) the data subject or a competent person where the data subject is a child consents to the processing;

c) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;

d) processing complies with an obligation imposed by law on Rotocon;

e) processing protects a legitimate interest of the data subject;

f) processing is necessary for the proper performance of a public law duty by a public body; or

g) processing is necessary for pursuing the legitimate interest of Rotocon or of a third party to whom the information is supplied.

9.3 In the event that Rotocon appoints or authorises an operator to process any personal information on its behalf or for any reason, it will implement necessary agreements to ensure that the operator or anyone processing personal information on behalf of Rotocon or an operator, must –

a) Process such information only with the knowledge or authorisation of Rotocon; and

b) Treat personal information which comes to his/her/its knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of his/her/its duties.

9.4 Rotocon must maintain the documentation of all processing operations under its responsibility.

10. Further Processing of Personal Information

10.1 Rotocon must ensure that the further processing of personal information be compatible with the purpose for which it was collected.

10.2 To assess whether further processing is compatible with the purpose of collection, Rotocon will take account of –

a) The relationship between the purpose of the intended further processing and the purpose for which the information was collected;

b) The nature of the information concerned;

c) The consequences of the intended further processing for the data subject;

d) The manner in which the information has been collected; and

e) Any contractual rights and obligations between the parties.

10.3 The further processing of personal information will not be incompatible with the purpose of collection if –

a) The data subject or competent person where the data subject is a child, has consented to the further processing of the information;

b) The information is available in or derived from a public record or has deliberately been made public by the data subject;

c) Further processing is necessary –

I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

IV. In the interest of national security;

d) The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to –

I. Public health or public safety; or

II. The life or health of a data subject or other individual(s);

e) The information is used for historical, statistical or research purposes and Rotocon ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

11. Retention and Restriction of Records

11.1 Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless –

a) The retention of a record is required or authorised by law;

b) Rotocon reasonably requires a record for lawful purposes related to its functions or activities;

c) Retention of a record is required by a contract between the parties thereto; or

d) The data subject or a competent person where the data subject is a child has consented to the retention of a record.

11.2 Information collected or processed initially for the purposes of historical, statistical or research value, may be retained for a period longer than contemplated in clause 10.1, providing Rotocon has appropriate measures in place to safeguard these records against uses other than what it was intended for initially.

11.3 Rotocon will destroy or delete a record of personal information or de-identify it as soon as reasonably practicably after Rotocon is no longer authorised to retain a record.

11.4 The de-identifying or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible/understandable form.

11.5 In the event that Rotocon uses a record of personal information of a data subject to make a decision about the data subject, it must –

a) Retain the record for such period as may be required or prescribed by law or a code of conduct; or

b) If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

11.6 Rotocon will restrict the processing of personal information if –

a) Its accuracy is contested by the data subject, for a period enabling Rotocon to verify the accuracy of the information;

b) Rotocon no longer needs the personal information for achieving the purpose for which it was collected or subsequently processed, but it has to be maintained for purposes of proof;

c) The processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

d) The data subject requests to transmit the personal data into another automated processing system.

11.7 Personal information that has been restricted may only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person where the data subject is a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

11.8 Where personal information is restricted, Rotocon will inform the data subject before lifting the restriction.

12. Security Safeguards

12.1 Rotocon will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent –

a) Loss of, damage to or unauthorised destruction of personal information; and

b) Unlawful access to or processing of personal information.

12.2 Rotocon will take responsible measures to –

a) Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

b) Establish and maintain appropriate safeguards against the risks identified;

c) Regularly verify that the safeguards are effectively implemented; and

d) Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

12.3 Rotocon will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

12.4 Rotocon will, in terms of a written contract between Rotocon and the operator, ensure that the operator which processes personal information for Rotocon, establishes and maintain the security measures as referred to in clause 12.1 – 12.3.

12.5 The operator will inform Rotocon immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

13. Security Compromises

13.1 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, Rotocon will notify –

a) The Information Regulator; and

b) The data subject, unless the identity of such data subject cannot be established.

13.2 The notification of a breach will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of Rotocon's information system.

13.3 Rotocon will only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

13.4 The notification to a data subject will be in writing and communicated to the data subject in at least one of the following ways:

a) Posted to the data subject's last known physical or postal address; or

b) Sent by e-mail to the data subject's last known e-mail address; or

c) Placed in a prominent position on the website of Rotocon; or

d) Published in the news media.

13.5 The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including–

a) A description of the possible consequences of the security compromise;

b) A description of the measures that Rotocon intends to take or has taken to address the security compromise;

c) A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

d) If known to Rotocon, the identity of the unauthorised person who may have accessed or acquired the personal information.

14. Rights of the Data Subject

14.1 The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information in terms of clause 9.2 (c) – (g), is not affected.

14.2 A data subject may object, at any time, to the processing of personal information–

a) In terms of clause 9.2 (c) – (g), in writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

b) For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

14.3 A data subject, having provided adequate proof of identity, has the right to –

a) Request Rotocon to confirm, free of charge, whether or not Rotocon holds personal information about the data subject; and

b) Request from Rotocon a record or a description of the personal information about the data subject held by Rotocon, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information –

I. Within a reasonable time;

II. At a prescribed fee as determined by the Information Officer;

III. In a reasonable manner and format; and

IV. In a form that is generally understandable.

14.4 A data subject may, in the prescribed manner, request Rotocon to –

a) Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

b) Destroy or delete a record of personal information about the data subject that Rotocon is no longer authorised to retain.

14.5 Upon receipt of a request referred to in clause 14.4, Rotocon will, as soon as reasonably practicable –

a) Correct the information;

b) Destroy or delete the information;

c) Provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or

d) Where an agreement cannot be reached between Rotocon and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

14.6 Rotocon will inform the data subject, who made a request as set out in clause 14.5, of the action taken as a result of the request.

15. Request for Disclosure

Rotocon will respond promptly when the data subjects request notification of purpose of use, disclosure, correction, addition or deletion of details, and suspension of use or elimination relating to personal information held by Rotocon.

16. Monitoring and Enforcement

Each employee of Rotocon will be responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedure, notices, consents and appropriate related documents and processes.

Managers and responsible employees will be trained according to their functions in legal requirements, policies and guidelines that govern the protection of personal information in Rotocon. Rotocon will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with privacy law and its policies, this Act and any applicable regulations. Employees who violate the guidelines and standard operating procedures of this policy may be subject to disciplinary action being taken against him/her.

17. Point of Contact

The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the handling, collection, processing or re-identifying of personal information shall be directed to the Information Officer or Deputy Information Officer(s) as referred to in the Information Officer Policy.

18. Standard Operating Procedures

Each department will establish appropriate privacy standard operating procedures that are consistent with this policy, local customs and practices as well as legal and regulatory requirements.

Duties and Responsibilities of Information Officer & Deputy Information Officer(s)

Policy	**Duties and Responsibilities of Information Officer & Deputy Information Officer(s)**
Applicable to	Information Officer & Deputy Information Officer(s)
Person responsible	Information Officer
Document No.	POL #

1. Appointment of Information Officer

The Information Officer in terms of Rotocon's structure will be the Chief Executive Officer.

2. Registration as Information Officer

The Information Officer shall ensure that he/she is registered with the Regulator within the prescribed manner and timeframe, as being the Information Officer of Rotocon.

3. Duties and Responsibilities of the Information Officer

The Information Officer's responsibilities include:

a) The encouragement of compliance with the conditions and stipulations of this Act for the lawful processing of personal information.

b) Dealing with requests made to Rotocon pursuant to this Act.

c) Working with the Regulator in relation to investigations conducted regarding the prior authorisation for processing, in relation to Rotocon.

d) Ensuring compliance by Rotocon with Rotocon's policies regarding the protection of personal information and the provisions of this Act.

4. Designations and Delegation of Deputy Information Officer(s)

4.1 The Information Officer may appoint any number of Deputy Information Officers as is necessary to perform the duties of the Information Officer as set out above. The Information Officer has control over every Deputy Information Officer(s) appointed.

4.2 The Information Officer may delegate, in writing, his/her power of duty conferred or imposed by this Act, to a Deputy Information Officer(s). In his/her decision to delegate power of duty, the Information Officer must give due consideration to the need to render Rotocon as accessible as reasonably possible for requests of its records.

4.3 The Deputy Information Officer's duties must only be exercised or performed subject to any conditions set by the Information Officer. The delegation of power does not prohibit the Information Officer from performing these duties himself/herself. The Information Officer may at any time withdraw or amend, in writing, the delegation of power of duty.

4.4 Any right or privilege acquired, or any obligation or liability incurred as a result of the delegation of power, is not affected by any subsequent withdrawal or amendment of that delegation.

5. Deputy Information Officer(s)

Name and Surname	Department	Date Appointed	Conditions

Prohibition on the Processing of Special Personal Information

Policy	**Prohibition on the Processing of Special Personal Information**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Prohibition on Processing of Special Personal Information

Rotocon will not process personal information, concerning –

a) The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

b) The criminal behaviour of a data subject to the extent that such information relates to –

I. The alleged commission by a data subject of any offence; or

II. Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

2. General Authorisation Concerning Special Personal Information

The prohibition on processing of special personal information, as referred to in clause 1 of this policy, does not apply if -

a) Processing is carried out with the consent of the data subject; or

b) Processing is necessary for the establishment, exercise or defence of a right or obligation in law; or

c) Processing is for historical, statistical or research purposes to the extent that –

I. The purpose serves a public interest and the processing is necessary for the purpose concerned; or

II. It appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent; or

d) Information has deliberately been made public by the data subject.

Prohibition on the Processing of Special Personal Information Regarding Data Subject's Race or Ethnic Origin

Policy	**Prohibition on the Processing of Special Personal Information Regarding Data Subject's Race or Ethnic Origin**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # (#)

1. Prohibition on the Processing of Special Personal Information

This policy should be read together with ***Policy #*** regarding the **Prohibition on the Processing of Special Personal Information**.

2. Authorisation Concerning a Data Subject's Race or Ethnic Origin

The prohibition on processing personal information concerning a data subject's race or ethnic origin, as referred to in ***Policy #*** regarding the **Prohibition on the Processing of Special Personal Information**, does not apply if the processing is carried out to –

a) Identify data subjects and only when this is essential for that purpose; and

b) Comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Prohibition on the Processing of Special Personal Information Regarding Data Subject's Health or Sex Life

Policy	**Prohibition on the Processing of Special Personal Information Regarding Data Subject's Health or Sex Life**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # (#)

1. Prohibition on the Processing of Special Personal Information

This policy should be read together with ***Policy*** **#** regarding the **Prohibition on the Processing of Special Personal Information**.

2. Authorisation Concerning Data Subject's Health or Sex Life

2.1 The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in ***Policy*** **#** regarding the Prohibition on the **Processing of Special Personal Information**, does not apply to the processing by –

a) Medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

b) Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for–

I. Assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing; or

II. The performance of an insurance or medical scheme agreement; or

III. The enforcement of any contractual rights and obligations;

c) Schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;

d) Any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;

e) Any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

f) Administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for –

I. The implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or

II. The reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

2.2 In cases referred to in clause 2.1, the information may only be processed by Rotocon subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between Rotocon and the data subject.

2.3 Where Rotocon is permitted to process information concerning a data subject's health or sex life in terms of this policy and is not subject to an obligation of confidentiality as referred to in clause 2.2, it must treat the information as confidential, unless Rotocon is required by law or in connection with its duties to communicate the information to other parties who are authorised to process such information in accordance with clause 2.1.

2.4 Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless –

a) A serious medical interest prevails; or

b) The processing is necessary for historical, statistical or research activity.

Prohibition on the Processing of Special Personal Information Regarding Data Subject's Criminal Behaviour or Biometric Information

Policy	**Prohibition on the Processing of Special Personal Information Regarding Data Subject's Criminal Behaviour or Biometric Information**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # (#)

1. Prohibition on the Processing of Special Personal Information

This policy should be read together with ***Policy*** # regarding the **Prohibition on the Processing of Special Personal Information**.

2. Authorisation Concerning Data Subject's Criminal Behaviour or Biometric Information

2.1 The prohibition on processing personal information concerning a data subject's criminal behaviour or biometric information, as referred to in ***Policy*** # regarding the **Prohibition on the Processing of Special Personal Information**, does not apply if the processing is carried out by bodies charged by law with applying criminal law or where Rotocon obtained that information in accordance with the law.

2.2 The processing of information regarding personnel in the service of Rotocon must take place in accordance with the rules established in compliance with labour legislation.

Processing Subject to Prior Authorisation

Policy	**Processing Subject to Prior Authorisation**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Processing Subject to Prior Authorisation

1.1 Rotocon must obtain prior authorisation from the Regulator, prior to any processing if Rotocon plans to –

a) Process unique identifiers of data subjects –

I. For a purpose other than the one for which the identifier was specifically intended at collection; and

II. With the aim of linking the information together with information processed by other responsible parties;

b) Process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

c) Process information for the purpose of credit reporting; or

d) Transfer special personal information or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

1.2 Rotocon will only have to obtain the prior authorisation once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised by the Regulator.

2. Rotocon to Notify the Regulator if Processing is Subject to Prior Authorisation

2.1 Rotocon must notify the Regulator when processing personal information referred to in clause 1.1 of this policy.

2.2 Rotocon may not carry out information processing that has been notified to the Regulator until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

Additional Policies:

Acceptable Use Policy

Policy	**Acceptable Use Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

The purpose of this policy is to direct all employees of Rotocon in the acceptable use and security of Rotocon's Internet Facilities. These standards contain directions for employees, indicating both acceptable and unacceptable Internet use with the aim of controlling employee behaviour and actions that contribute to Rotocon's Internet risks, while maximizing the benefits gained by Rotocon through Internet usage. As the software, hardware and computer network is the property of Rotocon it reserves the right to keep Rotocon and its systems secure through monitoring electronic information and regular checks on the system.

2. Roles and Responsibilities

2.1 Rotocon's Management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.

2.2 Rotocon's Management is responsible for implementing the requirements of this policy, or documenting non-compliance via the method described under exception handling.

2.3 Rotocon's Managers, in cooperation with the Information Officer, are required to train employees on policy and document issues with Policy compliance.

2.4 All of Rotocon's employees are required to read and acknowledge the reading of this policy by signing it.

3. Policy Directives

Part I - Management Requirements

1. Rotocon will establish formal Standards and Processes to support the on-going development and maintenance of Rotocon's Acceptable Use Policy.
2. Rotocon's Director(s) and Management will commit to the on-going training and education of Rotocon's staff responsible for the administration and/or maintenance and/or use of Rotocon's Internet facilities.
3. Rotocon's Director(s) and Managers will establish a formal review cycle for all Acceptable Use initiatives.
4. Any security issues discovered will be reported to the Information Officer or his Deputy Information Officers.

Part II – Ownership

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of Rotocon are the property of Rotocon and employee use of these files is neither personal nor private. The Information Officer may access all such files at any time without knowledge of the user or owner. Rotocon's management reserves the right to monitor and/or log all employee use of Rotocon's Information Resources with or without prior notice.

Part III – Acceptable Use Requirements

1. Employees will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
2. Employees must report any weaknesses in Rotocon's computer security to the appropriate security staff. Weaknesses in computer security include unexpected software or system behaviour, which may result in unintentional disclosure of information or exposure to security threats.
3. Employees must report any incidents of possible misuse or violation of this Acceptable Use Policy to the Information Officer.
4. Employees must not attempt to access any data, documents, email correspondence, and programs contained on Rotocon's systems for which they do not have authorization.
5. Employees must not attempt any access penetration tests, any investigations or perform any other activities to compromise the access controls of Rotocon's computing facilities, unless there is a demonstrated business requirement to do so and Rotocon's Manager has approved of such activities and the conditions under which it will apply in advance in writing.
6. Systems administrators and authorized users must not divulge remote connection modem phone numbers or other access points to Rotocon's computer resources to anyone without proper authorization in writing.

7. Employees must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
8. Employees must not make unauthorized copies of copyrighted software or software owned by Rotocon.
9. Employees must not use non-standard shareware or freeware software without the approval from Management.
10. Employees must not purposely engage in activity that may harass, threaten or abuse others or intentionally access, create, store or transmit material that Rotocon may deem to be offensive, indecent or obscene, or that is illegal in terms of applicable legislation.
11. Employees must not engage in activity that may degrade the performance of Information Resources; deprive an authorized user access to Rotocon's resources; obtain extra resources beyond those allocated; or circumvent Rotocon's computer security measures.
12. Employees must not download, install or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of Rotocon's computer resources unless approved by Information Officer.
13. Rotocon's Information Resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, or for the solicitation of performance of any activity that is prohibited by relevant legislation.
14. Access to the Internet from home based computers or computers owned by Rotocon, must adhere to all the policies. Employees must not allow family members or other non-employees to access non-public accessible computer systems of Rotocon.
15. Employees must not attempt to change the configuration of desktop computers and notebooks. All configuration changes must be handled by the IT department, for example upgrading operating systems, changing Windows settings, installing new software or systems, and installing modems, memory or storage upgrades.
16. In particular, Rotocon's Internet facilities may not be used for any of the following:
    - Communications in connection with the personal business interests of the user or the user's family.
    - Downloading, transmission, and possession of pornographic and sexually explicit materials.
    - Transmitting defamatory, slanderous, threatening and abusive messages, inflammatory statements, or any message that may be construed as such.
    - Political or religious statements, foul language, or any other statements viewed as harassing others based on race, creed, colour, age, sex, national origin, disability or physical attributes are prohibited.

- Unauthorized attempts to bypass or any attempt to circumvent any security mechanisms of computers connected to the Internet.
- Propagating, sending, responding to, redirecting, forwarding, or otherwise participating in chain letters or junk e-mail.
- The alteration, destruction, or infringement of the privacy of other employees' computer-based information residing on the Internet and e-mail systems.
- Playing computer games or engaging in any other form of entertainment or sporting activities during business hours.
- Any communications or activity, which could harm the good name and reputation of Rotocon.

17. Employees of Rotocon may not send or publish confidential and private material of Rotocon (internal memos, policies, etc.) on any publicly accessible or external Internet computer of Rotocon unless the owner of the information has first approved the publication of these materials.
18. Employees should not transmit confidential information, information of Rotocon, copyrighted materials, or any trade secrets of Rotocon over any public computer system or network unless properly protected through encryption methods.
19. Any security issues discovered will be reported to the Information Officer or his Deputy Information Officers.

Part IV – Incidental Use

1. Incidental personal use of electronic mail, Internet access, fax machines, printers, and copiers is restricted to Rotocon's approved users only and does not include family members or others not affiliated with Rotocon.
2. Occasional private use of Rotocon's Internet facilities are allowed under the following conditions:
   - Occasional and very short personal email communications by users are acceptable provided that they do not interfere with the users work and comply with the guidelines of this policy at all times. If the user is not sure whether a personal communication complies with the requirements of this policy, the prior authorization of the user's superior must be obtained before such messages are sent.
   - Personal use of Rotocon's Internet facilities must be kept to a minimum and in any event must not exceed 2 hours per week per user during office hours and 4 hours (1 hour at a time) per week after hours. Personal usage must not interfere with the user's work and such usage must comply with the requirements of this policy at all times.
3. Incidental use must not result in direct costs to Rotocon, cause legal action against, or cause embarrassment to Rotocon.

4. Incidental use must not interfere with the normal performance of an employee's work duties.
5. Storage of personal email messages, voice messages, files and documents within Rotocon's computer resources must be nominal.
6. Rotocon's Management will resolve incidental use questions and issues using these guidelines in collaboration with the Information Officer, HR Manager and the Line Manager/Supervisor.

4. Enforcement, Auditing, Reporting

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of Rotocon's Information Resources access privileges, civil, and criminal prosecution.
2. Rotocon's Management is responsible for the periodic auditing and reporting of compliance with this policy. Rotocon's Information Officer will be responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to Rotocon's Director(s).
3. Exceptions to this policy will be considered only when the requested exception is submitted in writing to the Information Officer.
4. Any employee may, at any time, anonymously report policy violations to the Information Officer.

E-mail Policy

Policy	**E-mail Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Introduction

Rotocon provides employees with electronic communication tools, including an e-mail system. This email policy, which governs employee use of Rotocon e-mail system, applies to e-mail use at Rotocon's premises and district offices, as well as remote locations, including, but not limited to, employee homes, airports, hotels, and client and supplier offices. Rotocon's e-mail rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates Rotocon's e-mail rules and policies is subject to disciplinary action, up to and including termination.

2. E-mail Exists for Business Purposes

Rotocon allows e-mail access primarily for business purposes. Employees may use Rotocon's e-mail system for personal use only in accordance with Rotocon's policies.

3. E-mail Monitoring Activities

Rotocon reserves the right to monitor, inspect, copy, review, and store any and all employee's e-mail use at any time and without prior notice. In addition, Rotocon may monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through Rotocon's e-mail system. Rotocon reserves the right to disclose e-mail information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.

4. Offensive Content and Harassing or Discriminatory Activities Are Banned

Employees are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

5. Employees Are Prohibited From Using E-mail to:

5.1 Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

5.2 Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

5.3 Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.

5.4 Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.

5.5 Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.

5.6 Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass Rotocon, negatively impact employee productivity, or harm employee morale.

6. Confidential, Proprietary, and Personal Information Must Be Protected

Unless authorized to do so, employees are prohibited from using e-mail to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about Rotocon, its employees, clients, suppliers, and other business associates. Confidential information includes, but is not limited to, client lists, credit card numbers, identification numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass Rotocon and its employees if the information were disclosed to the public.

7. Business Record Retention

E-mail messages are written business records and are subject to Rotocon's rules and policies for retaining and deleting business records. Please refer to Rotocon's Data Retention Policy for more information.

8. Information Exchange and Internet Transactions

8.1 All messages communicated on Rotocon's Internet and e-mail system must contain the employee's name. No e-mail or any other electronic communication may be sent which hides the identity of the sender or represents the sender as someone else. All emails sent must include the email signature of the sender.

8.2 Emails with attachments sent by employees may not exceed the limit as prescribed by the Information Officer.

8.3 The disclaimer as prescribed by the IT department must be used at the end of all email messages.

9. Violations

These guidelines are intended to provide Rotocon's employees with general examples of acceptable and unacceptable uses of Rotocon's e-mail system. A violation of this policy may result in disciplinary action up to and including termination.

Handheld & Mobile Device Policy

Policy	**Handheld & Mobile Device Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

This policy establishes rules for the proper use of handheld devices in Rotocon in order to protect the confidentiality of sensitive data, the integrity of data and applications, and the availability of services at Rotocon, protecting both handheld devices and their users, as well as corporate assets (confidentiality and integrity) and continuity of Rotocon.

2. Scope of application and obligations

This policy applies to all employees, consultants, vendors, contractors, students, and others using business or private mobile handheld devices on any premises occupied by Rotocon. Adherence to these requirements and the security policies derived from them and implementation of provisions is binding across the whole of Rotocon, its subsidiaries and majority holdings. Wilful or negligent infringement of the policies jeopardizes the interests of Rotocon and will result in disciplinary, employment, and/or legal sanctions. In the case of the latter the relevant line managers and where applicable legal services shall bear responsibility. These requirements and the security policies derived from them and implementation provisions also apply to all suppliers of Rotocon. They shall be contractually bound to adhere to the security directives. If a contractual partner is not prepared to adhere to the provisions, he must be bound in writing to assume any resulting consequential damage.

3. Roles & responsibilities

3.1 The IT department must ensure that all employees using devices falling into the category of “handheld devices” have acknowledged this security policy and the associated procedures before they are allowed to use corporate services using handheld devices.

3.2 The IT department must ensure that handheld devices and their users comply with this security policy and all security policies as stipulated by Rotocon.

3.3 Any employee found to have violated this policy is subject to disciplinary action, up to and including termination.

3.4 In a general sense, all users are required to use their common sense in order to act in the best interest of Rotocon, its assets and its services.

3.5 In case of doubt, users must contact the IT department to clarify a given situation.

3.6 Users of handheld devices must diligently protect such devices from loss and disclosure of private information belonging to or maintained by Rotocon.

3.7 Before connecting a mobile handheld device to the network at Rotocon, users must ensure it is on the list of approved devices issued by the IT department.

3.8 The IT department must be notified immediately upon suspicion of a security incident, especially when a mobile device may have been lost or stolen.

3.9 The cost of any item beyond the standard authorized equipment is the responsibility of the employee.

4. Exceptions to handheld security policy

Requests for an exception to this policy must be submitted to and approved by the Information Officer.

5. Use of private handheld devices

The Information Officer must define whether private handhelds are authorised to connect to Rotocon's networks.

5.1 Private handhelds are not authorised:

- In highly restricted facilities, private handheld devices must be prohibited. In that case, mobile devices must be collected prior to the user's entrance into the facility.
- Private handhelds are authorised in offices, but are not allowed to connect to internal networks.
- Private handhelds must not connect to Rotocon's networks and access corporate information. This includes synchronization with a workstation connected to the internal networks. Rotocon's networks must be protected accordingly using network access control mechanisms and must not grant access to any corporate information to unregistered devices.

5.2 Private handhelds are authorised:

- Any non-business-owned (private) device able to connect to Rotocon's network must first be approved by the IT department.
- If allowed, privately-owned handheld devices must comply with this policy and must be inventoried along with corporate handheld devices, but identified as private. This is in order to prevent theft of corporate data with unmanaged handhelds.

6. IT Department roles and responsibilities

6.1 The IT department is responsible for the mobile handheld device policy at Rotocon and shall conduct a risk analysis to document safeguards for each device type to be used on the network or on equipment owned by Rotocon.

6.2 This policy should be reviewed on an annual basis by the Information Officer and IT department of Rotocon, taking into account changes according to new services available, new capabilities of devices, changes in corporate backend servers, and new threats to mobile devices.

6.3 The IT department is responsible for developing procedures for implementing this policy.

6.4 The IT department maintains a list of approved mobile handheld devices and makes the list available on the intranet.

6.5 The IT department maintains a list of allowed and unauthorised applications.

7. User awareness training

7.1 Users must be trained in order to ensure the proper use of devices and resources of Rotocon. A focus on applications and basic security features of Rotocon is mandatory.

7.2 The following list is not exhaustive, but contains crucial points that must be treated during an initial training:

- Review of policies
- Procedure implementation
- Password protection
- How to deal with social engineering attacks
- Proper protection of devices
- Locking the device
- Preventing the use of systems by unauthorised users
- Protecting devices from loss or theft
- Ensuring the information on a handheld device is absolutely necessary
- Ensuring the information on a handheld device is also stored on Rotocon's network where it is regularly backed up
- How to encrypt sensitive information
- User awareness of changes in technologies and security policies should be regularly tested.

8. Inventory of mobile handheld devices

8.1 The IT department must keep inventory of handhelds in use in Rotocon, using associating owner names and identity for network access control.

8.2 The inventory must take into account at least but not limited to the following list of identifiers:

- Device name
- Owner's ID
- Device serial number
- Device IMEI
- Device's MAC address
- Owner's ID (user)
- User's MSISDN
- Device capabilities (Bluetooth, IrDA, Camera, etc.)
- Supplementary accessories provided

9. Authorised services and applications

9.1 Only approved third party applications may be installed on handhelds. The approved list can be obtained by contacting the IT department.

9.2 In the event that a desired application is not on the list, a request can be submitted to the IT department. If the program meets internal testing requirements of stability and security, it will be added and at that point it may be installed.

10. Forbidden devices

10.1 The IT department must provide a list of unauthorised applications and communicate it to the users.

10.2 The list of unauthorised applications must remain available to the users via the intranet.

10.3 The following services might be disabled according to Rotocon's risk analysis in order to prevent information disclosure or data leakage:

- Peer-to-peer services (e.g. Skype)
- MMS messages
- Instant messaging
- Camera
- Third-party applications

- Any type of tunnelling application that does not allow filtering the content of communications, except the approved VPN solution.

11. Unauthorised actions

11.1 Users must not modify security configurations without request to and approval by the IT department. Failure to comply with this rule will engage disciplinary procedures.

11.2 Unauthorised actions:

- Installing and/or using unauthorised applications or services
- Removing root certificates from certificate stores
- Conducting any careless actions leading to an interruption or service
- Disabling security features

12. Uncovered issues

All issues that are not covered by this security policy must be brought to the attention of the Information Officer or IT department of Rotocon, which will treat them on a case-by-case basis.

Access Control Policy

Policy	**Access Control Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

This policy establishes the guidelines for managing user access to information of Rotocon. The purpose is to ensure the necessary user access controls are in place for controlling the actions, functions, applications, and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all Rotocon's information resources.

All managers of Rotocon's information resources will ensure that access to Rotocon's information is properly authorized and granted with correct access levels and privileges applied.

2.1 Operational Definitions

2.1.1 "Authentication": Verification that the user's claimed identity is valid and is usually implemented through a user password at logon.

2.1.2 "Discretionary User Access": The ability to manipulate data using custom or general-purpose programs. The only information logged for discretionary control mechanisms is the type of data accessed and at what level of authority.

2.1.3 "Identification": The act of a user professing an identity to a system, usually in the form of a logon to the system.

2.1.4 "Non-discretionary User Access": The access obtained in the process of specific business transactions that affect information in a predefined way. For example, Rotocon's deployment specialists need to access participant information to make travel arrangements, but may not need the ability to change any existing information.

2.1.5 "Password": An arrangement of characters entered by a system user to substantiate their identity, authority, and access rights to an information system they wish to use.

2.1.6 "Privilege": The level of user authority or permission to access information resources. Privileges can be established at the folder, file, or application levels, or for other conditions as applicable.

2.1.7 "Special User Access Privileges": Privileges that allow users to perform specialized tasks that require broad capabilities. For example changing control functions such as: access control, logging, and violation detection, require special access privileges.

2.1.8 "User Account": An issued name with authority, granted to an individual to access a system or software application. System administrators, with proper management approval, typically grant accounts. To access an account, a user needs to be authenticated, usually by providing a password.

2.1.9 "User Access Controls": The rules and deployment of mechanisms, which control access in information resources, and physical access to premises.

2.2. User Accounts

The creation of a user account must be initiated through a request to the Information Officer who is authorised to approve access to the specified resources.

2.3 Account Management

Rotocon's IT department manages user accounts for Rotocon's systems. Records of processed and denied requests for creation of user accounts must be kept for auditing purposes. Records will be retained for one year, unless otherwise specified in the Data Retention Policy.

2.4 User Accounts Characteristics

All employee user accounts must be unique, and traceable to the assigned user. The IT department of Rotocon will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by the Director(s) of Rotocon.

2.5 Password Reset

The IT department of Rotocon will establish a procedure for verifying a user's identity prior to resetting their password.

2.6 User Account Privileges

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user's manager, and the evaluation of the Information Officer. The Information Officer has final determination as to the level of a user's access for their system.

2.7 Inactive Accounts

Accounts will be disabled after 30 days of inactivity. Users planning to deploy to field operating locations or to be away from the office for other approved periods of extended absence should be coordinated with the IT department in order to ensure proper disposition of the account.

2.8 Temporary User Accounts

All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created. Applications for temporary user accounts should be submitted for approval to the IT department.

2.9 Password Characteristics

All passwords must be constructed using the following characteristics: alphanumeric characters, with a mixture of letters, numbers and special characters. The IT department will implement appropriate procedures and technology to enforce this requirement.

2.10 Automatic Logon

The use of automatic logon software to circumvent password entry shall not be allowed, except with specific approval from the Information Officer, for special tasks such as automated backups.

2.11 User Account and Password Safekeeping

Each individual assigned a user account and password is responsible for the actions taken under said account, and must not divulge that account information to any other person for any reason.

2.12 Management of User Accounts

Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of Rotocon's information resources. The IT department will establish procedures for providing their management with access to accounts assigned to a user within their department. These procedures will be coordinated with the Director(s) and Information Officer.

2.13 Transfers

Personnel transferring from one area of responsibility to another shall have their access accounts modified to reflect their new job responsibilities.

2.14 User Access Cancellation

The IT department will implement procedures to immediately cancel account access and physical access for users whose relationship with Rotocon has concluded, either on friendly or unfriendly terms.

2.15 User Session Time-out

User sessions will time-out after the prescribed period of inactivity has lapsed, unless otherwise specified as part of the system or application security plan. This includes user connections to the Internet, or to specific applications.

2.16 Remote Access Security

Access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers.

2.17 New Information Systems

All new information systems acquired or developed by the IT department will incorporate access controls to properly protect Rotocon's information resources.

2.18 Sensitive Information Access

Individuals in positions with access to sensitive information will be screened for best suitability to the position. These individuals will be subject to the provisions of Rotocon's policies and procedures to protect and safeguard such information from unauthorised disclosure or access.

2.19 Temporary Access to Sensitive Resources

Temporary access to resources categorised as sensitive will be set with expiration dates where possible. The IT department will monitor temporary access to ensure activities comply with the intended purpose.

3. Applicability and Compliance

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within Rotocon's operating environment or connected to Rotocon's information infrastructure.

4. Responsibilities

4.1 Rotocon's Information Officer

The Information Officer will coordinate the implementation of this policy.

4.2 Rotocon's IT Department

The IT department will establish procedures to implement these requirements.

5. Program Implementation

The IT department will establish processes and procedures to implement this policy, and coordinate activities with the Information Officer.

5.1 User Access Administration

The Information Officer has primary management responsibility for administering user access to Rotocon's information resources.

Physical Security Policy

Policy	Physical Security Policy
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

All of Rotocon's premises that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, security guards, and fire protection.

2. Scope

This policy addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by Rotocon, including offices, data centres and similar facilities that are used to house such resources.

3. Policy

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

3.1 Use of Secure Areas to Protect Data and Information

Rotocon must use physical methods to control access to information processing areas. These methods include, but are not limited to, locked doors, secured cage areas, vaults, ID cards, and biometrics.

3.2 Physical Access management to protect data and information

Access to facilities that holds critical IT infrastructure, systems and programs must follow the principle of least privilege access. Employees, including full and part-time staff, contractors and vendors' staff should be granted access only to facilities and systems that are necessary for the fulfilment of their job responsibilities.

The process for granting physical access to information resources facilities must include the approval of the Information Officer, or his or her deputy. Access reviews must be conducted at least quarterly, or more frequently depending on the nature of the systems that are being protected. Removal of individuals who no longer require access must then be completed in a timely manner.

Access cards and/or keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.

Rotocon should ensure that visitors obtain security clearance before entering the premises. This could include, but is not limited to, a sign in book, employee escort within a secure area, ID check and ID badges for visitors.

Computers, printers and other non-portable information systems equipment belonging to Rotocon must not be removed from Rotocon's premises unless accompanied by an approved property pass issued by the IT Manager.

Equipment and media taken off premises should not be left unattended in public areas. Portable computers and personal digital assistants (PDA's) should be carried as hand luggage where possible when travelling.

4. Policy Notification

The Human Resources department of Rotocon is responsible for ensuring that employees are aware of where policies are located on websites. The Human Resources department is also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.

Anti-Virus Policy

Policy	**Anti-Virus Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

The purpose of this policy is to establish requirements which must be met by all computers connected to Rotocon's lab networks and to ensure effective virus detection and prevention.

2. Scope

This policy applies to all of Rotocon's computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers.

3. Policy

3.1 All of Rotocon's PC-based lab computers must have Rotocon's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. The IT department is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Rotocon's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

3.2 Users must not attempt to remove viruses themselves. If a virus infection is detected, users must disconnect from Rotocon's networks, stop using the infected computer immediately and notify the IT department.

3.3 Users must be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments. If a virus is suspected the attachment must not be opened or forwarded and must be deleted immediately.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Surveillance and Monitoring Policy

Policy	**Surveillance and Monitoring Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

The purpose of this policy is to prevent crime and assist Rotocon in protecting:

- The safety and property of Rotocon, its employees and visitors.
- The applicable legal and privacy interests of Rotocon, its clients and employees.

2. Scope

This policy applies to Business's, all permanent and temporary employees, contractors, consultants, including all personnel affiliated with third parties who use surveillance cameras in Rotocon and/or conduct surveillance monitoring and recording.

This policy does not apply to:

- The use of surveillance cameras or other surveillance conducts during criminal investigations, by Rotocon or by law enforcement agencies.

3. Definitions

3.1 Surveillance Camera

Any item, system, camera, technology device, communications device used alone or in conjunction with a network for the purpose of gathering, monitoring, recording or storing an image or images of Rotocon and/or people at the premises of Rotocon. Images captured by surveillance cameras may be real-time or preserved for review at a later date. Such devices may include, but are not limited to the following:

1. Close-circuit television
2. Web cameras
3. Real-time surveillance systems
4. Computerized visual monitoring
5. Cell phone with cameras

3.2 Surveillance Monitoring or Recording

Using surveillance cameras or other related technology to observe, review or store visual images for the purpose of deterring crime and protecting the safety and security of Rotocon.

3.3 Rotocon premises

All areas on property owned, leased or controlled by Rotocon, both internal and external, including offices, common spaces, and other areas.

4. Policy

Rotocon is committed to integrating the best security. Rotocon's use of surveillance cameras for surveillance monitoring or recording must be:

- Conducted in a professional, ethical, and legal manner.
- Compliant with Rotocon's Policies and Procedures.
- Limited to uses that does not violate a person's reasonable expectation of privacy, as defined by current legal requirements.

5. Procedures

5.1 Installation and/or placement of surveillance cameras in Rotocon premises must be approved by the Director(s)and Information Officer of Rotocon.

5.2 Only employees designated by the Director(s) and/or Information Officer will have access to the images captured by surveillance monitoring or recordings.

5.3 All existing uses of surveillance cameras and surveillance monitoring or recording, subject to this policy, must be in compliance with this policy. A request to continue using the existing surveillance cameras will be submitted to the Information Officer. Network connectivity for surveillance monitoring or recording must comply with Rotocon's policies.

5.4 Violations of these procedures may result in disciplinary action in accordance with the policies, contracts, rules and regulations of Rotocon.

6. Training

The Information Officer will ensure that the designated employees will be trained on the responsible use of the information and technology. Designated employees will also be supervised by a specific supervisor, with periodic review performed by the Information Officer or his/her deputy.

7. Retention and Release of Information

7.1 Rotocon will retain images obtained through surveillance monitoring or recording for a length of time deemed appropriate for the purpose of monitoring, but not to exceed 90 days, unless such images have historical value, or are being used for a criminal investigation. Any questions regarding the retention of these images should be directed to the Information Officer.

7.2 Only the Director(s) and Information Officer can authorize the release of information and results obtained through surveillance monitoring or recording.

7.3 The IT department will ensure that all networks are backed up regularly in order to ensure the safeguarding of personal information.

7.4 Information obtained in violation of this policy cannot be used in any disciplinary proceeding against any employee.

Data Retention Policy

Policy	Data Retention Policy
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

The purpose of this policy is to ensure that necessary records and documents of Rotocon are adequately protected and maintained to ensure that records that are no longer needed by Rotocon or are of no value, are discarded at the proper time. This policy is also for the purpose of aiding employees of Rotocon in understanding their obligations in retaining documents.

2. Scope

This policy applies to all documents which are collected, processed or stored by Rotocon and includes but is not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

3. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4. Guidelines for the Retention of documents

4.1 Rotocon may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. Employees will be notified of applicable documents where the destruction has been suspended to which they have access to.

4.2 All documentation and personal information that is being stored by Rotocon in accordance with this policy must be stored and guarded in compliance with all Rotocon's policies.

4.3 The documentation and information listed below may not contain all the records and documents processed and in the possession of Rotocon and should merely be used as a guideline.

4.4 In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed in accordance with the Data Destruction Policy of Rotocon.

4.5 The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

Accounting

Nr	**Type of document**	**Minimum Retention Required**
1	Annual Financial Statements including, annual accounts, director's and auditors report	15 Years
2	Books of accounting recording information required by the Companies Act No.71 of 2008	15 Years
3	Branch Register	5 Years
4	Certificate of change of name	Indefinite
5	Certificate of incorporation	Indefinite
6	Certificate to commence business	Indefinite
7	Director's attendance register	15 Years
8	Index of members	15 Years
9	Memorandum and articles of association	Indefinite
10	Minute book, CM25 and CM26, as well as resolutions passed at the general/class meetings	Indefinite
11	Microfilm image of any original record reproduced directly by the camera	Indefinite
12	Proxy forms	3 Years
13	Proxy forms used at court convened meetings	3 Years
14	Register of allotments – after a person ceased to be a member	15 Years
15	Register of directors and certain officers	15 Years
16	Register of director's shareholding	15 Years

17	Register of Members	15 Years
18	Register of mortgages and debentures and fixed assets	15 Years

Personnel Records

Nr	Type of document	Minimum Retention Required
1	Employee's employment contract	3 Years
2	Time worked by employee	3 Years
3	Remuneration to be paid to each employee	3 Years
4	Date of birth of any employee under 18 years of age	3 Years
5	Employee deduction authorisation	3 Years
6	Garnishments	3 Years
7	Employee disciplinary record	3 Years
8	Employee count records	3 Years

Health and Safety

Nr	Type of document	Minimum Retention Required
1	Register, records or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees compensated for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment, or for death sustained by these injuries at their place of work.	4 Years
2	A health and safety committee shall keep record of each recommendation 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.	3 Years

3	Records of incidents reported at work.	3 Years
4	Records of assessment and air monitoring, and the asbestos inventory.	Minimum of 40 years
5	Medical surveillance records	40 Years
6	Records of risk assessment and air monitoring results	40 Years
7	Medical surveillance records	40 Years
8	Records of assessment and air monitoring	30 Years
9	All records of assessments and noise monitoring	40 Years

Credit Agreements

Nr	Type of document	Minimum Retention Required
1	Enquiries	2 Years
2	Payment profile	5 Years
3	Adverse information	1 Year
4	Civil court judgements	The earlier of 5 years or until the judgement is rescinded by a court or abandoned
5	Administration orders	The earlier of 10 years or until the order is rescinded by a court
6	Sequestrations	The earlier of 10 years or the order is rescinded by a court
7	Liquidations	Unlimited
8	Rehabilitation orders	5 Years

Tax Records

Nr	Type of document	Minimum Retention Required

Electronic Communication

Nr	Type of document	Minimum Retention Required
1	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	As long as the information is used and at least 1 year thereafter
2	A Record of any third party to whom the information was disclosed	As long as information is used and at least 1 year thereafter
3	All personal data that has become obsolete	Destroy

Contracts

Nr	Type of document	Minimum Retention Required

Miscellaneous

Nr	Type of document	Minimum Retention Required
1	Employment record – all non-hired applicants (including all applications and resumes – whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence.	3 Years

Data Destruction Policy

Policy	**Data Destruction Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

The purpose of this policy is to provide guidance to Rotocon's employees regarding the destruction of documentation. All forms of computer equipment, digital storage media and printed or handwritten material must be disposed of securely when no longer required. Secure disposal maintains our data security and supports compliance with Rotocon policies and procedures.

Rotocon realises that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely and sees compliance of this policy as of the utmost importance in order to ensure that restricted data and/or personal information does not find its way into unauthorised hands.

2. Scope

This Policy aims to protect restricted data and personal information and applies to all users of Rotocon's network including Director(s), Manager(s), administrative personal, other employees, contractors, visitors and third parties. The Policy applies to all information systems owned by Rotocon and includes personal computers, Macs, laptops, mobile phones, handheld computers, servers and external or removable storage devices. The Policy also applies to printed materials.

3. Secure disposal

3.1 In determining whether a document and/or information should be stored or disposed of, each employee should first refer to the Data Retention Policy and in the event of any uncertainties, to the Information Officer of Rotocon.

3.2 Under no circumstances should paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.

3.3 Rotocon will ensure that all electrical waste, electronic equipment and data on disk drives be physically removed and destructed in such a way that the data will by no means be able to be virtually retrieved.

3.4 Employees must ensure that all paper documents that should be disposed of, be shredded locally within the department and then be recycled. Where local shredding is not possible, bulk quantities of restricted paper waste must be held in waste sacks. These will be collected and disposed of by an employee instructed to do so by the Information Officer.

3.5 In the event that a third party is used for data destruction purposes, this third party must also comply with the regulations as stipulated in this policy and any other applicable legislation.

Risk Management Policy

Policy	**Risk Management Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose and Scope

This policy establishes the process for the management of risks faced by Rotocon. The aim of risk management is to maximise opportunities in all Rotocon activities and to minimise adversity. The policy applies to all activities and processes associated with the normal operation of Rotocon. It is the responsibility of all Director(s), permanent and temporary employees to identify, analyse, evaluate, respond, monitor and communicate risks associated with any activity, function or process within their relevant scope of responsibility and authority.

2. Definitions

2.1 "Risk": is the likelihood that a harmful consequence (death, injury or illness) might result when exposed to a hazard. Risk is characterised and rated by considering two characteristics:

1. Probability or likelihood of occurrence; and
2. Consequence (C) of occurrence.

This is expressed as R (risk) = L (likelihood) x C (consequence).

2.2 "Likelihood": is a qualitative description of probability or frequency.

2.3 "Consequence": is the outcome of an event, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

2.4 "Risk control": means taking action to first eliminate health and safety risks so far as is reasonably practicable, and if that is not possible, minimising the risks so far as is reasonably practicable. Eliminating a hazard will also eliminate any risks associated with that hazard Risk Assessment is the process of evaluating and comparing the level of risk against predetermined acceptable levels of risk.

2.5 "Risk Management": is the application of a management system to risk and includes identification, analysis, treatment and monitoring.

2.6 "Risk Owner": is the person(s) responsible for managing risks and is usually the person directly responsible for the strategy, activity or function that relates to the risk.

3. Principles

Rotocon is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realised. Rotocon has the primary duty to ensure the health and safety of workers and other persons at the workplace.

4. Functions and Delegations

The Information Officer should exercise due diligence to ensure that **Rotocon** complies with the Protection of Personal Information Act and this Policy. This includes taking reasonable steps to:

- gain an understanding of the hazards and risks associated with the operations of **Rotocon;** and
- ensure that **Rotocon** has and uses appropriate resources and processes to eliminate or minimise risks to health and safety.

All Board members and employees must contribute to the establishment and implementation of risk management systems for all functions and activities of **Rotocon.** These risk management practices must align with all policies and applicable legislation.

5. Policy Detail

Rotocon aims to achieve better practice in the management of risks that threaten to adversely impact on **Rotocon** its functions, objectives, operations, assets, staff, consumers or members of the public. Rotocon does whatever it can (whatever is 'reasonably practicable') to ensure its workers, consumers and other people are not harmed by its activities**.**

6. Risk Management principles

Rotocon has to take into consideration the following aspects in adhering to risk management compliance:

- **Consulting with employees:**

It is imperative that the employees of Rotocon are made aware of the inherent risks that they are exposed to concerning their health and safety. It is important to have regular meetings with such employees in order to make sure that the employees have a thorough understanding of the processes and procedures in place to minimize such risk.

- **Identify hazards:**

Care should be taken in identifying the hazards associated with the day to day operations of Rotocon. These hazards include, but is not limited to the physical work environment, the equipment, materials and substances used, the work tasks and how they are performed. It is important to note the employees should be aware of these hazards as well as the precautions that need to be taken in order to minimize the potential damage.

- **How to assess risks:**

Your Consumer Protection legal advisor will assist in identifying the potential risk areas of Rotocon. He/she will also advise you on the appropriate measures to be implemented in order to minimize these risks.

- **How to control risks:**

It is important that upon identifying potential risk areas that appropriate measures be put in place in order to control and/or minimize those risk areas. Where it is possible for the hazard or risk to be eliminated completely, this should be done without delay. The responsible person who oversees this potential risk area must be made aware of such risk in order to implement appropriate safeguards.

- **How to review controls:**

It is important that Rotocon reviews the control measures in place to eliminate and minimize the risk areas on a regular basis.

- **How to keep records:**

It is essential that Rotocon documents and stores all applicable information regarding potential risk areas, as well as the decisions that was made and implemented in order to address those risk areas. These documents should be stored in accordance with the Data Retention Policy, as well as applicable legislation.

7. Role and Responsibility of the Information Officer

Rotocon has to take into consideration that the elected Information Officer needs to ensure that all employees, subcontractors, representatives, agents and suppliers have a reasonable understanding of the hazards and risks associated with the day to day responsibilities and operations in ensuring that Rotocon uses all appropriate resources and available processes to eliminate Rotocon's risk element.

Information Classification Policy

Policy	**Information Classification Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Purpose

It is critical for Rotocon to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, Rotocon has adopted this information classification policy to help manage and protect its information assets.

2. Responsibility

All of Rotocon's employees share in the responsibility for ensuring that Rotocon information assets receive an appropriate level of protection by observing this Information Classification policy:

- Managers of Rotocon or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below.('Owners" have approved management responsibility. 'Owners' do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All employees of Rotocon shall be guided by the information category in their security-related handling of Rotocon's information.

  All information of Rotocon and all information entrusted to Rotocon from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

Information Description	Examples	Category
Unclassified Public	Information is not confidential and can be made public without any implications for Rotocon.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available web site areas of Rotocon • Sample downloads of Rotocon's software that is for Sale • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Rotocon's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Rotocon activities • All software codes developed by Rotocon, whether used internally or sold to clients
Client Confidential Data	Information collected and used by Rotocon in the conduct of its businessto employ people, to log and fulfil clientorders, and to manage all aspects ofcorporate finance. Access to this informationis very restricted within Rotocon. Thehighest possible levels of integrity,confidentiality, and restricted availabilityare vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data and confidential contracts • Non-disclosure agreements with clients\vendors Company business plans

Disaster Recovery Policy

Policy	Disaster Recovery Policy
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL #

1. Roles and Responsibilities

The disaster recovery policy must be reviewed at least annually to assure its relevance, just as in the development of such a policy. A planning team that consists of upper management and personnel from the IT department, human resources, or other operations should be assembled to review the disaster policy. Roles and responsibilities of the planning team should be as follows:

- Perform an initial risk assessment to determine current information systems vulnerabilities.
- Perform an initial business impact analysis to document and understand the interdependencies among business processes and determine how Rotocon would be affected by an information systems outage.
- Take an inventory of information systems assets such as computer hardware, software, applications, and data.
- Identify single points of failure within the information systems infrastructure.
- Identify critical applications, systems, and data.
- Prioritize key business functions.

2. Implementation

Rotocon's personnel will carry out the following procedures in the implementation of the disaster recovery policy:

- Setup and maintain offsite facilities for data backup storage and electronic vaulting as well as redundant and reliable standby systems if necessary.
- Ensure that critical applications, systems, and data are distributed among facilities that are reasonably easy to get to but not so close that they could be affected by the same disaster.
- Establish written policies, contracts, and service level agreements with third party hosting, collocation, telecommunications, and Internet service providers that facilitate prompt recovery and continuity.

- Create an incident response team that consists of information security, IT, marketing, HR, legal, and other relevant personnel.
- Define the roles and responsibilities of the incident response team.
- Obtain each incident response team member's contact information.
- Determine which methods the incident response team members will use to communicate in the event of a disaster.
- Create a public relations officer to assist with the effective handling of an incident.
- Assign a manager (such as an IT Manager or Information Officer) that has the responsibility and authority to make critical IT decisions.
- Develop testing standards.
- Document and distribute the disaster recovery plan.
- Distribute copies of the written plans to everyone involved and also store extra copies in an offsite, fireproof vault.

3. Role and Responsibility of Information Officer

The following are on-going procedures that must be followed by employees and monitored by the Information Officer:

- Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
- Test plans at least annually, document and review the results, and update the plans as needed.
- Analyse plans on an on-going basis to ensure alignment with current business objectives and requirements.
- Provide security awareness and disaster recovery education for all team members involved.
- Continuously update information security policies and network diagrams.
- Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
- Perform continuous computer vulnerability assessments and audits.

Conclusion

The amendments have been compiled with the objective of guiding Rotocon to become compliant with the stipulations of the Protection of Personal Information Act, No 4 of 2013.

Resolution

The following policies and amendments applicable to Rotocon have been discussed and implimented at a meeting between the Information Officer and the Deputies (if applicable).

Date: _____

Signature: _____

Initials & Surname: _____

Designation: _____