RTT GROUP (PTY) LTD

REGISTRATION NUMBER 2014/020717/07

PROTECTION OF PERSONAL INFORMATION POLICY

TABLE OF CONTENTS

Clause number and description	Page

1. POLICY STATEMENT

1.1 Everyone has rights regarding how their personal information is handled. During the course of its activities RTT Group (Pty) Ltd will collect, store and process personal information about RTT Group (Pty) Ltd staff, customers, suppliers and other third parties. RTT Group (Pty) Ltd recognises the need to treat it in an appropriate and lawful manner.

1.2 **Any breach of this policy amounts to serious misconduct and may result in disciplinary action.**

2. RELEVANT DEFINITIONS

2.1 The following terms bear the meaning given to them here in this policy and its annexures:

2.1.1 "Data subjects" for the purpose of this policy include all living individuals and juristic persons about whom RTT Group (Pty) Ltd holds personal information. All data subjects have legal rights in relation to their personal information.

2.1.2 "**Operators**" include any person who processes personal information on behalf of a responsible party. Employees of responsible parties are excluded from this definition, but it could include suppliers which handle personal information on RTT Group (Pty) Ltd.'s behalf.

2.1.3 "**IO**" means the information officer appointed as such by RTT Group (Pty) Ltd in terms of section 56 of POPI and who will have the ultimate responsibility to ensure that RTT Group (Pty) Ltd complies with the provisions of POPI;

2.1.4 "**Personal information**" means information relating to an identifiable, living, natural person, and (where applicable) an identifiable, existing juristic person, including the name, race, gender, marital status, address and identifying number of a person, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person.

2.1.5 "**POPI**" means the Protection of Personal Information Act 4 of 2013.

2.1.6 "**Processing**" is any activity that involves use of personal information. It includes any operation or activity or any set of operations, whether by automatic means, concerning personal information, including—

2.1.6.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

2.1.6.2 dissemination by means of transmission, distribution or making available in any other form; or

2.1.6.3 merging, linking, as well as restriction, degradation, erasure or destruction of information.

2.1.7 "**Processing conditions**" are the 8 (eight) conditions for the lawful processing of personal information set out in chapter 3 of POPI.

2.1.8 "**Regulator**" means the Information Regulator established in terms of section 39 of POPI.

2.1.9 "**Responsible parties**" are the people who or organisations which determine the purposes for which, and the way, any personal information is processed. They have a responsibility to establish practices and policies in line with POPI. RTT Group (Pty) Ltd is the responsible party of all personal information used in its business.

2.1.10 "**Special personal information**" includes personal information concerning 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 the criminal behavior of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

2.1.11 "**Users**" include employees whose work involves using personal information. Users have a duty to protect the information they handle by always following RTT Group (Pty) Ltd.'s data protection and security policies.

3. ABOUT THIS POLICY

3.1 This policy applies to all users and will come into effect after the POPI compliance audit has been conducted.

3.2 The types of information that RTT Group (Pty) Ltd may be required to handle include details of current, past and prospective employees, customers, suppliers, contractors and others that RTT Group (Pty) Ltd communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in POPI and other regulations. POPI imposes restrictions on how RTT Group (Pty) Ltd may use that information.

3.3 This policy sets out RTT Group (Pty) Ltd.'s rules on personal information protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

3.4 Annexure C to this policy sets out a list of 'Do and Do Nots' under POPI.

3.5 This policy does not form part of any employee's contract of employment and may be amended at any time.

3.6 The IO is responsible for ensuring compliance with POPI and with this policy. That post is held by **Anje Lubbe , 011 552 1000, legal@rtt.co.za.** Any questions or concerns about the operation of this policy should be referred in the first instance to the IO.

3.7 If you consider that the policy has not been followed in respect of personal information about yourself or others you should raise the matter with your line manager or the IO.

4. PURPOSE OF THE POLICY

4.1 The purpose of the policy is to establish management direction and high-level objectives for regulating the way personal information is processed and to provide for remedies in cases where personal information is not handled accordingly. Further purposes of the policy include:

4.1.1 General Data Protection Regulation (GDPR) in line with South African laws;

4.1.2 compliance with the requirements of POPI;

4.1.3 the identification and codification of documents and ensuring adequate protection and maintenance of accuracy of documents where required;

4.1.4 providing a set framework and unified policy regarding the methods and procedures for the retention and destruction of documents;

4.1.5 ensuring records that are no longer required or documents that are of no value are destroyed properly and in accordance with the provision herein; and

4.1.6 providing assistance to employees in understanding the requirements relating to the protection of personal information and the retention and destruction of documents.

5. PROCESSING CONDITIONS

5.1 Anyone processing personal information must comply with the following eight processing conditions:

5.1.1 Condition 1: Accountability;

5.1.2 Condition 2: Processing Limitation;

5.1.3 Condition 3: Purpose Specification;

5.1.4 Condition 4: Further Processing Limitation;

5.1.5 Condition 5: Information Quality;

5.1.6 Condition 6: Openness;

5.1.7 Condition 7: Security Safeguards; and

5.1.8 Condition 8: Data Subject Participation.

Condition 1: Accountability

5.2 RTT Group (Pty) Ltd must ensure that the processing conditions are complied with.[1]

5.3 RTT Group (Pty) Ltd has appointed an IO to encourage and support RTT Group (Pty) Ltd's overall compliance with POPI.

5.4 The IO is responsible for drafting an information security policy, which will, among other things, address document retention, access to information and classification of data.

5.5 RTT Group (Pty) Ltd will furthermore designate specific individuals to monitor compliance with information security standards within each business area.

5.6 Training or awareness sessions for employees on information security will be conducted on a regular basis.

Condition 2: Lawfulness of processing

5.7 Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.[2]

5.8 This condition applies to electronic personal information and paper-based records stored in a non-automated filing system.

5.9 It is advisable to obtain voluntary, informed, and specific consent from data subjects, where possible, before collecting their personal information. (See the model consent clause in Annexure D.)

5.10 A data subject may withdraw consent at any time and such withdrawal of consent should be noted. A data subject may also object at any time on reasonable grounds, to the processing of its personal information, save if other legislation provides for such processing. RTT Group (Pty) Ltd may then no longer process the personal information.

[1] See section 6 of POPI.
[2] See section 10 of POPI.

Condition 3: Purpose specification

5.11 Personal information may only be processed for specific, explicitly defined, and legitimate reasons relating to the functions or activities of RTT Group (Pty) Ltd, of which the individual is made aware.[3]

5.12 Personal information will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any personal information which is not necessary for that purpose will not be collected in the first place.

5.13 Once collected, personal information will only be processed for the specific purposes notified to the data subject when the personal information was first collected or for any other purposes specifically permitted by POPI. This means that personal information will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the personal information is processed, the data subject will be informed of the new purpose before any processing occurs.

5.14 Records of personal information may only be kept for as long as necessary for achieving the purpose for which the information was collected or subsequently processed, unless:[4]

5.14.1 retention of the record is required or authorised by law;

5.14.2 the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

5.14.3 retention of the record is required by a contract between the parties thereto; or

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

5.15 Personal information will therefore not be kept longer than is necessary for the purpose for which it was collected. This means that personal information must be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form or be de-identified as soon as reasonably practicable after RTT Group (Pty) Ltd is no longer authorised to retain the record. For guidance on how long certain personal information is likely to be kept before being destroyed, contact the IO or see the Document Retention Policy set out in Annexure B.

---

[3] See section 13 of POPI.
[4] See section 14 of POPI.

Condition 4: Further processing limitation

5.16 Further processing of personal information must be compatible with purpose of collection, unless the data subject has consented to such further processing.[5]

5.17 Where personal information is transferred to a third party for further processing, the further processing must be compatible with the purpose for which it was initially collected.

5.18 If personal information is to be used for any other purpose the further consent of the data subject must be obtained. Where this is not possible, the IO should be consulted.

5.19 Personal information may only be disclosed to other recipients in accordance with the provisions of RTT Group (Pty) Ltd's Personal Information Sharing Policy attached as Annexure G.

Condition 5: Information quality

5.20 RTT Group (Pty) Ltd must take reasonably practicable steps to ensure that personal information is complete, accurate, not misleading and updated where necessary considering the purpose for which such information is collected.[6]

5.21 Information which is incorrect, or misleading is not accurate, and steps will therefore be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information will be destroyed.

5.22 The IO will develop processes for:

5.22.1 checking the accuracy and completeness of records containing personal information;

5.22.2 dealing with complaints relating to the timeliness and accuracy of personal information;

5.22.3 individuals to periodically verify and update their personal information;

5.22.4 making individuals aware of these processes; and

5.22.5 monitoring and tracking updates to personal information.

5.23 The IO will furthermore put procedures in place to verify that records containing personal information remain relevant, accurate and up-to-date.

---

[5] See section 15 of POPI.
[6] See section 16 of POPI.

Condition 6: Openness

5.24 RTT Group (Pty) Ltd must take reasonably practicable steps to ensure that the data subject is aware of[7]:

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

5.24.2 the name and address of RTT Group (Pty) Ltd;

5.24.3 the purpose for which the information is being collected;

5.24.4 whether or not the supply of the information by that data subject is voluntary or mandatory;

5.24.5 the consequences of failure to provide the information;

5.24.6 any particular law authorising or requiring the collection of the information;

5.24.7 where applicable, the fact that the responsible party intends to transfer the information to a country or international organisation and the level of protection afforded to the information by that country or international organisation;

5.24.8 any further information such as the recipient or category of recipients of the information, the nature or category of the information and the existence of the right of access to and the right to rectify the information collected;

5.24.9 the existence of the right to object to the processing of personal information; and

5.24.10 the right to lodge a complaint to the Regulator and the contact details of the Regulator,

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.

Condition 7: Security safeguards

5.25 RTT Group (Pty) Ltd will keep all personal information secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure and conduct regular risk assessments to identify and manage all reasonably foreseeable internal and external risks to personal information under its control.

[7] See section 18 of POPI.

5.26 RTT Group (Pty) Ltd will appoint a third-party specialist to secure the integrity of the personal information under RTT Group (Pty) Ltd.'s control.

Duty in Respect of Operators

5.27 Operators (i.e. third parties which may further process personal information collected by RTT Group (Pty) Ltd) include call centres, outsourced payroll administrators, marketing database companies, recruitment agencies, psychometric assessment centres, document management warehouses, external consultants, credit bureaus and persons who clear the payment instructions of RTT Group (Pty) Ltd.'s clients.

5.28 RTT Group (Pty) Ltd will implement the following key obligations in respect of operators:

5.28.1 The operator may not process personal information on behalf of RTT Group (Pty) Ltd without the knowledge and authorisation of RTT Group (Pty) Ltd;

5.28.2 RTT Group (Pty) Ltd will ensure that the operator implements the security measures required in terms of Condition 7: Security Safeguards;

5.28.3 There will be a written contract in place between RTT Group (Pty) Ltd and the operator which requires the operator to maintain the confidentiality and integrity of personal information processed on behalf of RTT Group (Pty) Ltd;

5.28.4 The written contract between RTT Group (Pty) Ltd and the operator will include the provisions set out in Annexure E hereto; and

5.28.5 If the third party is located outside of South Africa, RTT Group (Pty) Ltd will consult the IO.

5.29 The use of any Closed-Circuit Television (CCTV) to monitor and record activities for the purposes of safety and security will comply with the provisions of the CCTV Policy (attached hereto as Annexure I.)

Duties in Respect of Security Compromises

5.30 In the event that personal information has been compromised, or if there is a reasonable belief that a compromise has occurred, RTT Group (Pty) Ltd (or an operator processing personal information on its behalf) will comply with the Security Compromises Policy (attached hereto as Annexure J.)

Condition 8: Data subject participation

Request for Information

5.31 RTT Group (Pty) Ltd recognises that a data subject has the right to request RTT Group (Pty) Ltd to confirm, free of charge, whether or not it holds personal information about the data subject and request RTT Group (Pty) Ltd to provide a record or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information at a prescribed fee.[8]

5.32 All users will comply with RTT Group (Pty) Ltd.'s Subject Access Request Policy attached hereto as Annexure H in respect of any access to personal information requests by data subjects.

Request to Correct or Delete

5.33 The data subject may request RTT Group (Pty) Ltd's IO to:

5.33.1 correct or delete personal information relating to the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, misleading, or obtained unlawfully; or

5.33.2 destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

5.34 RTT Group (Pty) Ltd will provide credible proof to the individual of the action that has been taken in response to the request.

5.35 If any changes to the personal information will have an impact on any decisions to be made about the individual, RTT Group (Pty) Ltd will inform all third parties to whom the information has been disclosed, including any credit bureaus, of such changes.

6. FAIR AND LAWFUL PROCESSING

6.1 POPI is intended not to prevent the processing of personal information, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For personal information to be processed lawfully, certain requirements have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the responsible party or the party to whom the personal information is disclosed. In most cases when special personal information is being processed, the data subject's explicit consent to the processing of such information will be required.

6.3 Personal information about users may be processed for legal, personnel, administrative and management purposes and to enable the responsible party (i.e. RTT Group (Pty) Ltd) to meet its legal

[8] See section 23 of POPI.

obligations as an employer, for example to pay users, monitor their performance and to confer benefits in connection with their employment. Examples of when special personal information of users is likely to be processed are set out below:

6.3.1 information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

6.3.2 the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with employment equity legislation; and

6.3.3 in order to comply with legal requirements and obligations to third parties.

6.4 Personal information about customers, suppliers and other third parties may be processed for the following purposes:

6.4.1 legal – such as handling claims, complying with regulations, or pursuing good governance and Client on boarding and verification;

6.4.2 service delivery– such as providing, supporting and enhancing services, processing by third parties and where applicable cross-border transfers;

6.4.3 business – such as internal audit, fraud prevention, reporting, accounting, credit checks, business planning, improvement or other proposed and actual transactions.

7. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

7.1 Personal information will be processed in line with data subjects' rights. Data subjects have a right to:

7.1.1 request access to any personal information held about them by a responsible party;

7.1.2 prevent the processing of their personal information for direct marketing purposes;

7.1.3 ask to have inaccurate personal information amended; and

7.1.4 object to any decision that significantly affects them being taken solely by a computer or other automated process.

8. PROVIDING INFORMATION TO THIRD PARTIES

8.1 Users dealing with enquiries from third parties should be careful about disclosing any personal information held by RTT Group (Pty) Ltd. In particular they should:

8.1.1 check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

8.1.2 suggest that the third party puts their request in writing so the third party's identity and entitlement to the information may be verified;

8.1.3 refer to the IO for assistance in difficult situations; and

8.1.4 where providing information to a third party, do so in accordance with the eight processing conditions.

9. MONITORING AND REVIEW OF THE POLICY

This policy is reviewed annually by the IO to ensure it is achieving its stated objectives.

Annexure A – POPI Audit Questionnaire

RTT GROUP (PTY) LTD

PROTECTION OF PERSONAL INFORMATION ACT

COMPLIANCE SURVEY

PLEASE READ THE FOLLOWING GUIDANCE NOTES BEFORE COMPLETING THIS FORM:

- The Protection of Personal Information Act 4 of 2013 (POPI) was signed into law by the President on 19 November 2013. As an employee of RTT Group (Pty) Ltd you are well aware that we have always been committed to quality and compliance with industry standards and applicable laws. POPI exposes RTT Group (Pty) Ltd and, indeed, all parties who process personal information of data subjects to potential liability.
- The purpose of this questionnaire is to find out what personal information RTT Group (Pty) Ltd / your department collects and how that information is used to enable RTT Group (Pty) Ltd to set standards for compliance with POPI.
- Please complete this form in full and do not leave any blanks.

BUSINESS DIVISION/DEPARTMENT												
NAME AND DESIGNATION OF PERSON COMPLETING QUESTIONNAIRE												
COMPLETION DATE	D	D	M	M	Y	Y	Y	Y				
PART I – GENERAL COLLECTION AND PROCESSING PROVISIONS									**Y**	**N**	**N/A**	
1. Does your department collect, receive, record, organise, collate, store, update, modify, retrieve, alter, consult, use, transmit, distribute, make available in any other form, merge, link, restrict, degrade, erase, or destroy, any information relating to the following categories?												
	Y	**N**	**N/A**		**Y**	**N**	**N/A**		**Y**	**N**	**N/A**	
RACE				**SEXUAL ORIENTATION**				**BELIEF**				

GENDER				AGE				CULTURE			
OTHER				TELEPHONE NUMBER				BIRTH			
PREGNANCY				WELLBEING				EDUCATION			
MARITAL STATUS				DISABILITY				COLOUR			
NATIONALITY				RELIGION				UNIQUE IDENTIFIER			
ETHNICITY				CONSCIENCE				E-MAIL ADDRESS			
ETHNIC OR SOCIAL ORIGIN				PHYSICAL OR MENTAL HEALTH				PHYSICAL ADDRESS			
MEDICAL, FINANCIAL, CRIMINAL OR EMPLOYMENT HISTORY				LOCATION INFORMATION				BIOMETRIC INFORMATION			
PERSONAL OPINIONS, VIEWS OR PREFERENCES				THE VIEWS OR OPINIONS OF ANOTHER INDIVIDUAL ABOUT THE DATA SUBJECT (THE PERSON TO WHOM INFORMATION RELATES)				CORRESPONDENCE SENT BY A PERSON THAT IS IMPLICITLY OR EXPLICITLY OF A PRIVATE / CONFIDENTIAL NATURE			
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											
FINANCIAL OR CREDIT HISTORY											

1.1. Please specify whether such information is stored as manual or computer files and whether it is readily accessible by your department.			
1.2. Please specify the reason(s) or purpose(s) for collecting such information (i.e. why is it necessary to collect and process such information / what objective does collection and processing achieve?)			
1.3. Please specify whether the person to whom the information relates is made aware of the reason for collecting such information.			
1.4. Please specify whether the information is used for any further purposes.			
1.5. Please specify whether any information is sent outside the borders of South Africa.			
1.6. Please specify the period that each item is retained for.			
1.7. If any of such information is destroyed, please advise as to: • The period of retention before destruction; • The reason for destruction; • The manner of destruction; • If the information is destroyed by a third party, please specify the manner of destruction and the third party details and whether a contractual agreement exists between your unit/the business and the third party.			
1.8. Do you have a process in place to ensure the completeness and accuracy of such information both during collection and at all stages thereafter?	**YES**	**NO**	**N/A**
1.9. If the answer to 1.8 is "**yes**", please describe this process.			
1.10. Is any information processed by a third party on your behalf? (Please note that this applies to all information referred to in 1.1. and includes information marked "no" or "not applicable".)	**YES**	**NO**	**N/A**
1.11. If the answer to 1.10 is "**yes**", please specify the items, the processing third party and whether there is an existing contract in place with the third party.			
1.12. Do you process any information on behalf of a third party? (Do you assist any person, juristic or natural, in entering into a contract with a third party or collect any information on the third party's behalf?)	**YES**	**NO**	**N/A**
1.13. If the answer to 1.12 is "**yes**", please specify the items, the third party(s) on whose behalf the information is processed and whether there is an existing contract in place with the third party.			

PART II – RIGHTS OF DATA SUBJECTS AND PROCESSING CONDITIONS			
2. Is voluntary, specific and informed consent requested and obtained from the person to whom the information relates before such information is collected or used?	YES	NO	N/A
2.1. If the answer to 2 is "**yes**", please specify how such consent is obtained and attach documentary proof where possible.			
2.2. Is all such information collected directly from the data subject?	YES	NO	N/A
2.3. If the answer to 2.2 is "**yes**", is any of the information verified by an independent source, such as TransUnion ITC?			
2.4. If the answer to 2.2 is "**no**", please specify the nature of the information and its source.			
2.5. Is the privacy and security of the information collected sufficiently protected both during collection and at all stages thereafter, i.e. are there security safeguards in place to protect the information?	YES	NO	N/A
2.6. If the answer to 2.5 is "**yes**", please specify how such information is protected, your response should indicate what safeguards are in place, how risks are identified and managed, what controls are in place and how often the efficacy of these controls is reviewed. Your response should also make specific reference to: • Maintaining the integrity and confidentiality of personal information; • The technical and organisational measures employed; • Prevention of unauthorised destruction ; • Prevention of unauthorised duplication; • Prevention of unlawful access ; and • Other relevant risks and how these are mitigated.			
2.7. If the answer to 2.5 is "**no**", please specify how the privacy or security of such information may actually or potentially be compromised.			
2.8. Is direct marketing sent to persons by means of emails, faxes or SMSes and the like?	YES	NO	N/A
2.9. Are data subjects afforded an opportunity to object to their personal information being used for purposes of direct marketing/unsolicited electronic communications?	YES	NO	N/A
2.10. If the answer to 2.9 is "**yes**", please specify how such objection is noted and enforced.			

2.11. Are data subjects afforded an opportunity to object to the use of their personal information on reasonable grounds relating to their particular situation?	YES	NO	N/A
2.12. If the answer to 2.11 is "**yes**", please advise how such objection is noted and enforced.			
2.13. Do you conduct security checks (identity verification) before divulging personal information relating to any person to any other third party?	YES	NO	N/A
2.14. If the answer to 2.14 is "**yes**", please provide full details of the following**:** • How security checks are conducted; and • The rules governing security checks, including, the number of questions asked, the types of questions asked and the degree of variance allowed/disallowed.			
2.15. Do you receive requests for copies of information or the deletion of information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully?	YES	NO	N/A
2.16. If the answer to 2.15 is "**yes**", do you action these requests?	YES	NO	N/A
2.17. If the answer to 2.16 is "**yes**", please provide full details of how these requests are actioned and how the information is provided or deleted or amended in your department and throughout all the departments.			

Annexure B– Document Retention Policy

RTT GROUP (PTY) LTD

DOCUMENT MANAGEMENT POLICY

1. DEFINITIONS

1.1. "**Destruction Authorities**" means permission granted by the **Retention Manager** for the destruction of certain data, information or records, in whichever form;

1.2. "**IO**" means the information officer appointed in terms of PAIA and / or POPI;

1.3. "**Non-Regulated Documents**" means documents, data, information or records that need to be retained for commercial purposes and so identified by RTT Group (Pty) Ltd, fully detailed in Appendix B hereto;

1.4. "**PAIA**" means the Promotion of Access to Information Act 2 of 2000;

1.5. "**POPI**" means the Protection of Personal Information Act 4 of 2013;

1.6. "**Regulated Document**" means all the documents, records and information detailed in Appendix A hereto;

1.7. "**Retention Committee**" means the committee body responsible for creating a document retention policy and for its implementation;

1.8. "**Retention Schedule**" means the document setting out the retention periods for relevant data, information or records, as provided for in the policy on record retention and / or destruction.

1.9. "**User(s**)" means all employees employed by RTT Group (Pty) Ltd and includes RTT Group (Pty) Ltd's directors, contract workers and the officer in charge of retention.

2. APPLICATION

This Document Management Policy should be read in conjunction with RTT Group (Pty) Ltd's policy on record retention and / or destruction which, collectively, apply to all Users and, in certain circumstances, apply to suppliers and customers of RTT Group (Pty) Ltd.

3. PURPOSE

The purpose of this policy is to supplement RTT Group (Pty) Ltd policy dealing with record retention and / or destruction to ensure that RTT Group (Pty) Ltd complies with document-retention provisions contained in applicable legislation ("regulatory compliance").

4. CREATION OF DOCUMENT MANAGEMENT ARCHIVE

4.1. As soon as reasonably possible after his/her appointment, the officer in charge of retention shall ensure that an archive for RTT Group (Pty) Ltd is constructed.

4.2. The archive may be:

4.2.1. In physical (i.e. paper) format.

4.2.2. In electronic format, provided that all the electronic records may only be stored onto the categories of storage medium prescribed by the Retention Committee and which meets the prescripts of the Retention Committee and Electronic Communications and Transactions Act 25 of 2002;

4.2.3. Outsourced to a third-party service provider, provided all the requirements in terms of RTT Group (Pty) Ltd's policy on record retention and / or destruction are met; and/or

4.2.4. A combination of the above.

4.3. RTT Group (Pty) Ltd may decide to encompass the different ways of storing documents, depending on the type of document or record. It is advisable that the most cost-effective methods are used.

4.4. The legal requirements and aspects (not an extensive list) of electronic storage are highlighted in Appendix C attached to this policy.

5. MANAGEMENT OF REGULATED DOCUMENTS

5.1. All Regulated Documents (as detailed in Appendix A) that are created, received or handled by Users shall be forwarded to the officer in charge of document retention for archiving.

5.2. The [officer in charge of document retention] shall, upon receipt of the relevant Regulated Document, allocate an index number to the document and retain the document in the archive for the period detailed in Appendix A.

6. MANAGEMENT OF NON-REGULATED DOCUMENTS

6.1. All Non-Regulated Documents (as detailed in Appendix B) that are created, received or handled by Users shall be forwarded to the officer in charge of document retention for archiving.

6.2. The officer in charge of document retention shall, upon receipt of the relevant Non-Regulated Document, allocate an index number to the document and retain the document in the archive for the period detailed in Appendix B.

7. NAMING STANDARDS

7.1. The officer in charge of document retention shall inform all Users of the indexing standards and all Users shall apply such standards in the creation and classification of RTT Group (Pty) Ltd documents.

7.2. The indexing standards should be objectively ascertainable from the face of the indexing standards document and should not rely on the specific and personal knowledge of any one person, including the officer in charge of document retention, to be comprehensible.

8. USER DUTIES

8.1. Users shall not destroy documents or any form of data if such document or data falls in the categories detailed in Appendices A and B and without Destruction Authorities.

8.2. Documents falling within the categories of Appendices A and B shall be forwarded by hand or electronic mail to the officer in charge of document retention for retention.

9. E-MAIL DESTRUCTION

9.1. Users shall, on the last day of every month, delete all personal or non- RTT e-mail messages (incoming and outgoing as well as attachments thereto) from the User's e-mail programme. This is to as to avoid email congestion.

9.2. Users shall save and retain all e-mail messages (which have been assessed to determine whether it contains a record that needs to be retained as required by RTT Group (Pty) Ltd's policy on record retention and / or destruction in a folder and for a period as specified in the Retention Schedule.

10. DISPOSAL AND DESTRUCTION OF DOCUMENTS AND RECORDS

10.1. Documents or records that are not required to be kept in terms of either regulatory or non-regulatory prescriptions should be destroyed.

10.2. Regulatory Documents shall only be destroyed if the periods detailed in Appendix A have lapsed, subject to the approval of the officer in charge of document retention. Non-Regulatory Documents shall only be destroyed if the periods detailed in Appendix B have lapsed, subject to the approval of the officer in charge of document retention.

10.3. Duplicates and copies, when the originals are available and intact, should be destroyed.

10.4. Shredding of documents or records is the best option available for the destruction of such documents, especially confidential documents, whilst burning poses environmental and safety problems which will require additional safety and other measures to be complied with.

11. ELECTRONIC INFORMATION MANAGEMENT

Where the Retention Committee in charge of and overseeing retention policy and implementation decides to manage and retain documents and records electronically, in whole or in part, the officer in charge of document retention shall see to the construction of an electronic archive that shall comply with and address the "retention", "original" and "evidence" requirements of the Electronic Communications and Transactions Act 25 of 2002 as detailed in Appendix C1 hereto and which shall be sufficiently secure.

12. PROTECTION OF PERSONAL INFORMATION

12.1. POPI places an obligation upon RTT Group (Pty) Ltd, as a responsible party, to collect, use and destroy personal information in a responsible and accountable way.

12.2. "Personal information" is broadly defined in POPI to include a range of information relating to an identifiable, living, natural person, as well as an identifiable, existing juristic person, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity.

12.3. RTT Group (Pty) Ltd will collect and store personal information for lawful purposes which are related to the functions and business activities of RTT Group (Pty) Ltd, and such purposes will be compatible with and necessary to pursue and maintain the legitimate interests of RTT Group (Pty) Ltd. Personal information may also be processed by RTT Group (Pty) Ltd for the purposes of management, research, analysis, corporate reporting and improving business efficiencies.

12.4. RTT Group (Pty) Ltd will take steps to ensure that its suppliers and customers are made aware of the specific purpose/s for which RTT Group (Pty) Ltd collects and processes the personal information of a supplier or customer, and will furthermore destroy, delete or de-identify a record of the personal information of a supplier or customer as soon as reasonably practicable after RTT Group (Pty) Ltd is no longer authorised to retain such record.

12.5. RTT Group (Pty) Ltd will collect and store the personal information of Users, suppliers and customers in physical and/or electronic form, as the circumstances require.

12.6. RTT Group (Pty) Ltd will always endeavour to secure the integrity and confidentiality of personal information which is in its possession or under its control.

12.7. Users and other data subjects have the right at any time to request that RTT Group (Pty) Ltd confirms the personal information which it holds about Users, and to request that RTT Group (Pty) Ltd corrects any incorrect or inaccurate personal information which it holds about a User.

12.8. In accordance with POPI, records of personal information will not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

12.8.1. Retention of the record is required or authorised by law;

12.8.2. RTT Group (Pty) Ltd reasonably requires the record for lawful purposes related to its functions or activities;

12.8.3. Retention of the record is required by a contract between the parties thereto; or

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

12.9. It is therefore important to consider the document-retention periods in the various statutes that may be applicable to RTT Group (Pty) Ltd (see Appendix A). Please note that this list is not exhaustive and may be updated from time to time as required.

13. GENERAL REMARKS AND OFFENCES

13.1. It should be noted that once litigation commences, or where litigation is reasonably expected, all records which could reasonably become subject to discovery proceedings or relevant to the dispute must be retained. A court can draw negative inferences or impose penalties for improper destruction of records. Furthermore, if evidence relevant to litigation or pending litigation is destroyed it may constitute an obstruction of justice.

13.2. PAIA provides that where access to records is requested in terms of PAIA, a person who with the intent to deny such right, destroys, damages or alters a record; conceals a record; or falsifies a record; or makes a false record, commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding 2 (two) years. As a result, RTT Group (Pty) Ltd will take steps to ensure that it at all times remains in compliance with its obligations under PAIA, and all other applicable law.

14. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for RTT Group (Pty) Ltd and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

15. POLICY REVISION

This policy has been reviewed and approved by the IO and is subject to change without prior notice.

CONTACT DETAILS OF THE IO

Name: Anje Lubbe
Address: C/O SPRINGBOK & JONES ROAD BARTLETT BOKSBURG
E-mail address: Legal@rtt.co.za
Telephone number: 011 552 1000

APPENDIX A

DOCUMENTS THAT SHOULD BE RETAINED IN TERMS OF LEGISLATION AND ACCEPTED INDUSTRY STANDARDS ("Legally Required Documents")

BASIC CONDITIONS OF EMPLOYMENT ACT 75 OF 1997 ("BCEA")	
APPLICATION AND GENERAL REMARKS	
The BCEA prescribes minimum employment conditions and standards for employees.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. Every employer must supply an employee, when the employee commences employment, in writing with the particulars set out in section 29.[9]	3 years from the date of the last entry in the record or after the termination of employment.
2. Every employer must keep a record containing at least the following information under the BCEA:[10] i. the employee's name and occupation; ii. the time worked by each employee; iii. remuneration paid to each employee; iv. the date of birth of any employee who is under the age of 18 (eighteen) years of age.	7 years.
3. In order to monitor or enforce compliance with an employment law, a labour inspector may— i. require a person to disclose information, either orally or	

[9] Section 29 of the BCEA. See also section 33(1) which concerned information an employer must give an employee on each day the employee is paid.
[10] See section 31 of the BCEA.

	in writing, and either alone or in the presence of witnesses, on any matter to which an employment law relates, and require that the disclosure be made under oath or affirmation; ii. inspect, and question a person about, any record or document to which an employment law relates; iii. copy any record or document referred to in section 66(b), or remove these to make copies or extracts; iv. require a person to produce or deliver to a place specified by the labour inspector any record or document referred to in paragraph (b) of section 66 for inspection; v. inspect, question a person about, and if necessary remove, any article, substance or machinery present at a place referred to in section 65; vi. inspect or question a person about any work performed; and vii. perform any other prescribed function necessary for monitoring or enforcing compliance with an employment law.	

COMPENSATION FOR OCCUPATIONAL INJURIES AND DISEASES ACT 130 OF 1993 ("COIDA")	
APPLICATION AND GENERAL REMARKS	
COIDA provides for compensation for disablement caused by occupational injuries or diseases sustained or contracted by employees in the course of their employment, or for death sustained from these injuries at their place of work.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
The following documents should be retained: i. Payrolls; ii. Accident books and records; iii. Salary revision schedules; iv. Staff records; v. Time and piecework records; vi. Wage and salary records (including overtime details). vii. The Director-General of the Department of Labour may subpoena any person who in his opinion is able to give information concerning the subject of any inquiry in terms of COIDA, or who is suspected to have or in the opinion of the Director-General has in his possession or custody or under his control any book, document or thing which has a bearing on the inquiry, to appear before him at a time and place specified in the subpoena, to be interrogated or to produce such book, document or thing, and the Director-General may retain such book, document or thing for further investigation. viii. A person authorized by the Director-General may— ix. without previous notice, at all reasonable times enter any premises;	7 years.

x. while he is on the premises, or at any time thereafter, question any person who is or was on the premises; xi. order any person who has control over or custody of any book, document or thing on or in those premises to produce to him forthwith, or at such time and place as may be determined by him, such book, document or thing; xii. at any time and place order any person who has the possession or custody of or is in the control of a book, document or thing relating to the business of an employer or previous employer, to produce forthwith or at such time and place as may be determined by him, such book, document or thing; xiii. seize any book, document or thing which in his opinion may serve as evidence in any matter in terms of this Act; xiv. examine or cause to be examined any book, document or thing produced to him or seized by him, and make extracts therefrom or copies thereof, and order any person who in his opinion is qualified thereto to explain any entry therein; xv. order an employee to appear before him at such time and place as may be determined by him, and question that employee.	

THE COMPANIES ACT 71 OF 2008 ("Companies Act")	
APPLICATION AND GENERAL REMARKS	
The Companies Act consolidates the law that regulates all companies operating in South Africa. Records, when used with respect to any information pertaining to a company, are classified in the Companies Act as any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act or any other public regulations.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC[11]**
1. A copy of the Memorandum of Incorporation and the rules of the company.	Life of the company.
2. A profit company must also maintain a securities register, or its equivalent as prescribed in the Act.	Life of the company.
3. Every public company that appoints a company secretary, auditor and audit committee has to maintain a record of its company secretaries and auditors. If this person is an individual, then the person's name and former name if applicable and his or her date of appointment must be recorded. Where a firm or juristic person is appointed, the name, registration number and registered office address of that firm or juristic person as well as the name of the individual determined by that firm per section 44(1) of the Auditing Profession Act 26 of 2005 to be responsible for performing the functions of auditor, must be recorded. Any changes in these	No timeframe provided in relation to the retention of these records and it is generally assumed that it should be kept for the life of the company.

[11] Section 24 of the Companies Act provides that records should be kept in a written, or other form, or manner, that allows that information to be converted into written form within a reasonable time.

particulars must be recorded as they occur, with the date and nature of such change.[12]	
4. Record of current and past directors, including, in respect of each director:	
i. full name and former names (if any);	7 years after the past directors have retired from the company.
ii. identity number, or, if the person does not have one, his or her date of birth;	
iii. nationality and passport number, if the person is not South African;	
iv. occupation;	
v. date of his or her most recent election or appointment as director of the company;	
vi. the name and registration number of every other company or foreign company of which the person is a director and in the case of a foreign company, the nationality of that company.	7 years after the event or meeting occurred.
5. Copies of all reports presented at annual general meetings of the company, annual financial statements and accounting records.	7 years after the date each such resolution was adopted.
6. Notice and minutes of all shareholders' meetings, including all resolutions adopted by them and any document that was made available by the company to the holders of securities in relation to such resolution.	7 years after the date on which such communication was issued.
7. Copies of all written communications sent generally by the company to all holders of any class of the company's securities.	7 years after the date of each such meeting during which such resolution was adopted.
8. Minutes of all meetings and resolutions of directors or directors' committees or the audit committee.	

[12] See section 26 of the Companies Act.

PRESCRIPTION ACT 68 OF 1969 ("Prescription Act")	
APPLICATION AND GENERAL REMARKS	
The Prescription Act consolidates and amends the laws relating to prescription.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
It is advisable, but not mandatory, to retain bills of exchange.[13]	6 years.

[13] See section 11(C) of the Prescription Act – the debt in relation to a bill of exchange prescribes after 6 years.

TAX ADMINISTRATION ACT 28 OF 2011 ("Tax Administration Act")
APPLICATION AND GENERAL REMARKS
The Tax Administration Act provides for the effective and efficient collection of tax, the alignment of the administration provisions of the tax Acts (including the Income Tax Act 58 of 1962 and the Value Added Tax Act 89 of 1991) and the consolidation of the provisions into one piece of legislation to the extent practically possible. The requirements of the Tax Administration Act to keep records, books of account or documents for a tax period apply to a person who has submitted a return for the tax period; is required to submit a return for the tax period and has not submitted a return for the tax period; or is not required to submit a return but has, during the tax period, received income, has a capital gain or capital loss, or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.[14] The records, books of account, and documents must be kept or retained in their original form in an orderly fashion and in a safe place; in the form, including electronic form, as may be prescribed by the Commissioner of Tax in a public notice; or in a form specifically authorised by a senior South African Revenue Services ("**SARS**") official.[15]

DOCUMENT[16]	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
A person must keep the records, books of account or documents that enable the person to observe the requirements of a tax Act; are specifically required under a tax Act or by the Commissioner of Tax by public notice; and enable SARS to be satisfied that the person has observed these requirements.	5 years from the date of the submission of the return or from the end of the relevant tax period, as the case may be.

[14] See section 29(2) of the Tax Administration Act.
[15] See section 30 of the Tax Administration Act.
[16] See section 29 of the Tax Administration Act.

VALUE-ADDED TAX ACT 89 OF 1991 ("VAT ACT")	
APPLICATION AND GENERAL REMARKS	
The VAT Act provides for the taxation of the supply of goods and services as well as the importation of goods and services.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. In addition to the records required under the Tax Administration Act the following documents should be retained by a VAT vendor:[17] i. A record of all goods and services supplied by or to the vendor showing the goods and services, the rate of tax applicable to the supply and the suppliers or their agents, in sufficient detail to enable the goods and services, the rate of tax, the suppliers or the agents to be readily identified by the Commissioner of Tax, and all invoices, tax invoices, credit notes, debit notes, Company statements, deposit slips, stock lists and paid cheques relating thereto; ii. A record of all importations of goods and documents relating thereto; iii. Documentary proof, as is acceptable to the Commissioner of Tax, substantiating the vendor's entitlement to a deduction at the time a return in respect of the deduction is furnished; iv. The charts and codes of account, the accounting instruction manuals and the system and programme documentation which describe the accounting system used in each tax period in the supply of goods and services; v. Any debtor and creditor list required to be prepared where a	5 years (calculated from the date of the last entry or from the date of completion of the transaction).

[17] See section 55(1) of the VAT Act.

vendor's basis of accounting is changed in accordance with the VAT Act;[18] vi. Any documentary proof required to be obtained and retained where a rate of zero per cent has been applied by any vendor.[19]	

[18] See section 15 (9) of the VAT Act.
[19] See section 11(3) of the VAT Act.

LABOUR RELATIONS ACT 66 OF 1995 ("LRA")	
APPLICATION AND GENERAL REMARKS	
The LRA governs the relations between employers, employees, registered trade unions and registered employers' organizations and provide a framework for collective bargaining between the parties. The Act further stipulates that various records should be retained for future reference.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
1. Registered trade unions and registered employers' organisations must preserve each of its books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, and auditor's reports, in an original or reproduced form.[20]	3 years from the end of the financial year to which they relate.
2. With each monthly remittance in terms of section 13, the employer must give the representative trade union[21]—	
i. employer has made the deductions that are included in the remittance;	Indefinitely.
ii. details of the amounts deducted and remitted and the period to which the deductions relate; and	3 years from the end of the financial year to which they relate.
iii. a copy of every notice of revocation.	3 years from the date of every ballot.
iv. a list of the names of every member from whose wages the An employer must disclose to a trade union representative all relevant information that will allow the trade union	

[20] See section 98(4) of the LRA.
[21] Section 13(5) of the LRA.

representative to perform effectively the functions under this Act.[22]	3 years from the date of the event or end of the period to which they relate.
3. Every registered employers' organisation must keep:	
i. a list of their members;	
ii. the minutes of their meetings, in an original or reproduced form; and	3 years from the date of the event or end of the period to which they relate.
iii. the ballot papers.	
4. Employers must keep prescribed details regarding the following matters:[23]	
i. strikes, lock-outs or protest action involving their employees;	
ii. records of each employee, specifying the nature of any disciplinary transgressions, the action taken by the employer and the reasons for such action.	
5. Every employer must keep the records that an employer is required to keep in compliance with an applicable collective agreement, and an arbitration award. An employer must submit those records in response to a demand made by a bargaining council, commissioner or any person whose functions in terms of the LRA include the resolution of disputes.[24]	

[22] Section 16(2) of the LRA. Section 21(1) of the LRA also provides that an employer must disclose to the commissioner any information and facilities that are reasonably necessary for the commissioner to determine the membership or support of the registered trade union and section 89 provides that an employer must disclose to the workplace forum all relevant information that will allow the workplace forum to engage effectively in consultation and joint decision making.
[23] See section 205 of the LRA.
[24] Id.

THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 ("ECTA")	
APPLICATION AND GENERAL REMARKS	
ECTA regulates electronic communication and prohibits the abuse of information. The Act provides conditions for the electronic collection of personal information and also for the timeframe that this information must be retained. All personal data that has become obsolete must be destroyed.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
The following information must be kept: 1. personal information and the specific purpose for which the data was collected must be retained (by the person who electronically requests, collects, collates, processes or stores the information); and 2. a record of any third party to whom the information was disclosed.	As long as such information is used and at least 1 year thereafter.

THE CONSUMER PROTECTION ACT 68 OF 2008 ("CPA")	
APPLICATION AND GENERAL REMARKS	
The CPA applies to the promotion of goods and services, the supply of goods and services in terms of a transaction and the goods and services themselves. Document retention requirements are prescribed in relation to promotional competitions.	
DOCUMENT	**PERIOD OF RETENTION** **ORIGINAL OR ELECTRONIC**
The promoter of a promotional competition must retain:[25] 1. full details of the promoter, including identity or registration numbers, as the case may be, addresses and contact numbers; 2. the rules of the promotional competition; 3. a copy of the offer to enter into a promotional competition; 4. the names and identity numbers of the persons responsible for conducting the promotional competition; 5. a full list of all the prizes offered in the promotional competition; 6. a representative selection of materials marketing the promotional competition or an electronic copy of such marketing materials; 7. a list of all instances when the promotional competition was	3 years.

[25] See regulation 11 of GNR.293 of 1 April 2011: Regulations (Government Gazette No. 34180).

marketed, including details on the dates, the medium used and places where the marketing took place; 8. the names and identity numbers of the persons responsible for conducting the selection of prize winners in the promotional competition; 9. an acknowledgment of receipt of the prize signed by the prize winner, or legal guardian where applicable, and his or her identity number, and the date of receipt of the prize, or proof by the promoter that the prize was sent by post or other electronic means to the winner using his or her provided details; 10. declarations made under oath or affirmation by the persons responsible for conducting the promotional competition that the prize winners were to their best knowledge not directors, members, partners, employees, agents or consultants of or any other person who directly or indirectly controls or is controlled by the promoter or marketing service providers in respect of the promotional competition, or the spouses, life partners, business partners or immediate family members; 11. the basis on which the prize winners were determined; 12. a summary describing the proceedings to determine the winners, including the names of the persons participating in determining the prize winners, the date and place where that determination took place and whether those proceedings were open to the general public; 13. whether an independent person oversaw the determination of the prize winners, and his or her name and identity number; 14. the means by which the prize winners were announced and the frequency of such announcements; 15. a list of the names and identity numbers of the prize winners; 16. a list of the dates when the prizes were handed over or paid	

to the prize winners; 17. in the event that a prize winner could not be contacted, the steps taken by the promoter to contact the winner or otherwise inform the winner of his or her winning a prize; 18. in the event that a prize winner did not receive or accept his or her prize, the reason for his or her not so receiving or accepting the prize, and the steps taken by the promoter to hand over or pay the prize to that prize winner.	

THE FOLLOWING ACTS, AS AND WHEN APPLICABLE, IMPOSE INDIRECT REPORTING/DISCLOSURE OBLIGATIONS		
Employment Equity Act 55 of 1998	Section 18(1) Section 26	When a designated employer engages in consultation in terms of this Act the employer must disclose to the consulting parties all relevant information that will allow those parties to consult effectively. An employer must establish and, for the prescribed period, maintain, records in relation to its workforce, its employment equity plan and any other records relevant to its compliance with this Act.
Competition Act 89 of 1998	Section 49A	At any time during an investigation in terms of the Act, the Competition Commissioner may summon any person who is believed to be able to furnish any information on the subject of the investigation, or to have possession or control of any book, document or other object that has a bearing on that subject- (a) to appear before the Commissioner or a person authorised by the Commissioner, to be interrogated at a time and place specified in the summons; or (b) at a time and place specified in the summons, to deliver or produce to the Commissioner, or a person authorised by the Commissioner, any book, document or other object specified in the summons.

	Section 54	The member of the Competition Tribunal presiding at the hearing may (a) direct or summon any person to appear at any specified time and place; (b) question any person under oath or affirmation; (c) summon or order any person i. to produce any book, document or item necessary for the purpose of the hearing; ii. to perform any other act in relation to this Act.
Promotion of Access to Information Act 2 of 2000	Section 50	A requester must be given access to any record of a private body if- (a) that record is required for the exercise or protection of any rights; (b) that person complies with the procedural requirements in this Act relating to a request for access to that record; and (c) access to that record is not refused in terms of any ground for refusal contemplated in PAIA. A request contemplated in subsection (1) includes a request for access to a record containing personal information about the requester or the person on whose behalf the request is made.
Unemployment Insurance Act 63 of 2001	Section 56	Every employer must as soon as it commences activities as an employer provide information regarding its employees to the commissioner.
Labour Relations Act 66 of 1995	Section 189(3)	When an employer contemplates dismissing one or more employees for reasons based on the employer's operational requirements, the employer must issue a written notice inviting the other consulting party to consult with it and disclose in writing all relevant information. An employer that is facing financial difficulties that may reasonably result in the winding-up or sequestration of the employer, must advise

	Section 197B	consulting parties and an employer that applies to be wound up or sequestrated must at the time of making application, provide consulting parties with a copy of the application.

NO STATUTORY GUIDANCE – STANDARD PRACTICE	PERIOD OF RETENTION*
DOCUMENT	**ORIGINAL OR ELECTRONIC****
The following documents should be retained:	
1. General contracts – indemnities and guarantees	5
2. Licensing agreements	5
3. Rental and hire purchase agreements	5
4. General legal correspondence	3
5. Accounting related correspondence	5
6. Negotiations	5
7. Unsuccessful job applications	1
8. Insurance claims and accident reports (after date of settlement)	5
9. Patent related agreements and records	3
10. Trademark related agreements and records	5
	5
	5
	10
	5

*** Periods are "years" unless indicated otherwise**

** **See requirements in Appendix C in respect of electronic records.**

APPENDIX B

DOCUMENTS THAT SHOULD BE RETAINED BY THE COMPANY

FOR COMMERCIAL PURPOSES ("Commercially Required Documents")

INFORMATION THAT SHOULD BE RETAINED FOR COMMERCIAL PURPOSES	**PERIOD OF RETENTION**
DOCUMENT	**ORIGINAL AND/OR ELECTRONIC RETENTION**
The following documents should be retained by 1. Accounting /Investment Records; 2. Contracts and Agreements; 3. Correspondence; 4. Electronic Data; 5. Employee Records; 6. Insurance Records; 7. Pension Records; 8. Property Records; 9. Share Registration Records; and 10. Statutory Records.	As per Appendix A

APPENDIX C

REQUIREMENTS FOR ELECTRONIC RECORDS MANAGEMENT

Where a law requires information to be retained, that requirement is met by retaining such information in electronic format, if -

- the information contained electronically is accessible so as to be usable for subsequent reference;
- the data in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- the origin and destination of that data and the date and time it was sent or received can be determined.

APPENDIX C1

REQUIREMENTS TO "RETAIN" DOCUMENTS IN ELECTRONIC FORMAT

SECTION 16 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if -

a) the information contained in the data message is accessible so as to be usable for subsequent reference;

b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

APPENDIX C2

REQUIREMENTS TO ARCHIVE "ORIGINAL" DOCUMENTS IN AN ELECTRONIC ARCHIVE

SECTION 14 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if -

a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity must be assessed -

a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

b) in the light of the purpose for which the information was generated; and

c) having regard to all other relevant circumstances.

APPENDIX C3

REQUIREMENTS TO ARCHIVE EVIDENCE IN ELECTRONIC FORMAT

SECTION 15 OF THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence -

a) on the mere grounds that it is constituted by a data message; or

b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to -

a) the reliability of the manner in which the data message was generated, stored or communicated;

b) the reliability of the manner in which the integrity of the data message was maintained;

c) the manner in which its originator was identified; and

d) any other relevant factor.

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

ANNEXURE C– POPI - "Do and Do Nots"

1. DOs

1.1. DO conduct an information retention audit by creating a matrix which clearly identifies the various categories of personal information held by each department of RTT Group (Pty) Ltd, including emails, and setting out a precise retention policy for each category. (The POPI Audit Questionnaire in 0 should be used for this purpose.)

1.2. DO designate someone as an IO and ensure this person is adequately trained and registered with the Regulator.

1.3. DO, where possible, obtain "voluntary, specific and informed" consent from a data subject, including customers of RTT Group (Pty) Ltd, prior to processing his information, including his name, race, gender, marital status, address, identity number, e-mail address, physical address, and telephone number.

1.4. DO assume that RTT Group (Pty) Ltd will probably only have one chance to obtain the prescribed consent.

1.5. DO ensure that RTT Group (Pty) Ltd obtains "optimum" consent.

1.6. DO remember that POPI applies to paper files, information held electronically, video/DVD, audiotapes, photographs, images recorded on CCTV cameras, biometric information such as fingerprints etc.

1.7. DO be careful about sensitive data, namely data concerning race, political opinion, religious belief, trade union membership, physical or mental health, sex life, and criminal offences.

1.8. DO ensure the integrity and safekeeping of personal information in RTT Group (Pty) Ltd's possession or under its control, by among other things, taking steps to prevent the information being lost, damaged, or unlawfully accessed.

1.9. DO define the purpose of gathering and processing of information, collect personal information only for a specific, explicitly defined and lawful purpose that is related to a function or activity of RTT Group (Pty) Ltd, and hold personal information only when necessary.

1.10. DO process personal information in a lawful manner; personal information is processed lawfully when if it is adequate, relevant, and not excessive given the purpose for which it is processed.

1.11. DO take steps to notify the data subject that RTT Group (Pty) Ltd holds personal information about him and tell him why RTT Group (Pty) Ltd needs to do so.

1.12. DO check the rationale for any further processing and ensure further processing is compatible with the purpose for which the data was initially collected.

1.13. DO ensure that RTT Group (Pty) Ltd has a written contract (data processing agreement) in place when sharing personal information with other organisations or third parties and that these parties enter into a Non-Disclosure Agreement.

1.14. DO ensure that personal information is entered into records accurately and that the information is complete, up to date, and not misleading.

1.15. DO obtain parental consent when collecting personal information about persons under the age of 18.

1.16. DO ensure that any paper record is properly filed or disposed of.

1.17. DO accommodate data subject requests, including requests to disclose the identity of all third parties that have had access to their information (which request RTT Group (Pty) Ltd must execute free of charge) and provide a record of personal information (which request RTT Group (Pty) Ltd may execute at a reasonable fee).

1.18. DO hold personal information in such a way that it can be collected for inspection at short notice.

1.19. DO direct any official requests to see personal information to the IO.

1.20. DO, as far as possible, de-identify (anonymise) personal information for statistical analysis.

1.21. DO respect the rights of a data subject, which include the right to confidentiality, which requires that RTT Group (Pty) Ltd refuses requests from family, friends and employers for information about him, including references, unless the written consent of the data subject has been acquired.

1.22. DO retain records for required periods only as personal information must be destroyed, deleted, or "de-identified" as soon as the purpose for collecting the information has been achieved, unless it is a requirement of law to keep it for a longer period. A record of the information must be retained, however, if RTT Group (Pty) Ltd has used it to make a decision about the data subject, including the CVs of prospective employees, for long enough for the data subject to request access to it. (Refer to the Document Retention Policy in 0.)

1.23. DO review personal information kept in files and dispose of unnecessary information as confidential waste.

1.24. DO consider providing "open references" for employees leaving RTT Group (Pty) Ltd only (which are shown to the employee before they are sent to third parties).

1.25. DO, when writing documents, bear in mind that the data subjects have a right to see information relating to them.

1.26. DO note that transborder data transfer (including to neighbouring countries) is stringently regulated; therefore, seek further advice from the IO when this is to be done.

1.27. DO process personal information for the purpose of direct marketing by means of any form of electronic communication only if the data subject has given its consent to the processing or is a customer of RTT Group (Pty) Ltd.

1.28. DO process the personal information of a data subject who is a customer of RTT Group (Pty) Ltd for direct marketing purposes only:

1.28.1. If RTT Group (Pty) Ltd has obtained the contact details of the data subject in the context of the 'sale' of a service;

1.28.2. for the purpose of direct marketing of RTT Group (Pty) Ltd's own similar services; and

1.28.3. if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of its electronic details at the time when the information was collected and in each subsequent communication.

1.29. DO approach a data subject whose consent is required and who has not previously withheld such consent only once in order to request the consent of that data subject.

1.30. DO request the data subject's consent in the prescribed manner and form once such manner and form have been prescribed (presumably in Regulations to be published in future under POPI).

1.31. DO include in any communication for the purpose of direct marketing:

1.31.1. details of the identity of RTT Group (Pty) Ltd; and

1.31.2. an address or other contact details to which the recipient may send a request that such communications cease (i.e. include an opt-out function).

1.32. DO make sure that any opt-outs are recorded appropriately.

1.33. DO take special care when accessing RTT Group (Pty) Ltd.'s computer network remotely and ensure that data is encrypted.

2. DO NOTs

2.1. DO NOT ignore POPI. Ignorance may lead to a civil action for damages, regardless of whether intent or negligence can be proven on the part of RTT Group (Pty) Ltd, and to an enforcement notice being issued by the Regulator (non-compliance with an enforcement notice is an offence).

2.2. DO NOT use old mailing lists.

2.3. DO NOT reveal personal information to third parties without the data subject's permission or justification.

2.4. DO NOT take up references without the consent of the data subject, i.e. only ever approach individuals named by the data subject.

2.5. DO NOT verify qualifications of employees or job seekers without the consent of the data subject.

2.6. DO NOT hold personal information about a person without explicit consent or advice from the IO.

2.7. DO NOT print personal information without a good reason.

2.8. DO NOT place personal information about an individual on the Internet without his/her permission, unless it is a condition of his/her employment.

2.9. DO NOT send personal information outside South Africa (including our neighbouring countries) without taking advice from the IO.

2.10. DO NOT leave personal information insecure in any way, whether it is physical files or information held electronically.

2.11. DO NOT allow staff to take personal information (such as credit checks) home without particular care for security.

2.12. DO NOT process personal information on a computer that is not owned or supplied by RTT Group (Pty) Ltd.

2.13. DO NOT part with RTT Group (Pty) Ltd's computers without advice on deletion of data from the IO.

2.14. DO NOT use email for sending confidential communications or unencrypted personal information, as it is relatively insecure.

2.15. DO NOT use personal information held for one purpose for a different purpose without permission from the data subject.

2.16. DO NOT delete or alter any personal information after the IO has received a request to inspect and/or disclose that personal information.

2.17. DO NOT mention anything in email correspondence that RTT Group (Pty) Ltd would not want a data subject to see; even deleted emails may be retrieved and revealed to those about whom they are written.

ANNEXURE D– Model POPI Consent Clause

Processing of Personal Information

The Client's privacy is very important to RTT Group (Pty) Ltd and it will use reasonable efforts in order to ensure that any information, including personal information, provided by the Client, or which is collected from the Client, is stored in a secure manner.

The Client agrees to give (where applicable) honest, accurate and current information about the Client to RTT Group (Pty) Ltd and to maintain and update such information when necessary.

The Client's personal information collected by RTT Group (Pty) Ltd may be used for the following reasons:

- legal – such as handling claims, complying with regulations, or pursuing good governance and Client on boarding and verification;
- service delivery– such as providing, supporting and enhancing services, processing by third parties and where applicable cross-border transfers;
- business – such as internal audit, fraud prevention, reporting, accounting, credit checks, business planning, improvement or other proposed and actual transactions.

The Client acknowledges that any information supplied to RTT Group (Pty) Ltd in terms of these Terms of Business is provided voluntarily.

By submitting any information to RTT Group (Pty) Ltd in any form the Client further acknowledges that such conduct constitutes an unconditional, specific and voluntary consent to the processing of such information by RTT Group (Pty) Ltd under any applicable law in the manner contemplated above, which consent shall, in the absence of any written objection received from the Client, be indefinite and/or for the period otherwise required in terms of any applicable law.

Unless the Client has consented, RTT Group (Pty) Ltd will not sell, exchange, transfer, rent or otherwise make available any personal information about the Client (such as name, address, email address, telephone or fax number) to other parties and the Client indemnifies RTT Group (Pty) Ltd from any unintentional disclosures of such information to unauthorized persons.

Should the Client believe that RTT Group (Pty) Ltd has utilised the Client's personal information contrary to applicable law, the client shall first resolve any concerns with RTT Group (Pty) Ltd. If the Client is not satisfied with such process, the Client has the right to lodge a complaint with the Regulator, once established.

ANNEXURE E – Model POPI Operator Clauses

1. Definitions

1.1. **"Agreement"** means this written services agreement between RTT Group (Pty) Ltd and the Operator;

1.2. **"Data Subject"** shall have the meaning ascribed to it in Chapter 1 of POPI;

1.3. **"Operator"** shall have the meaning ascribed to it in Chapter 1 of POPI;

1.4. **"Parties"** means the parties to this Agreement being, together, RTT Group (Pty) Ltd and the Operator and "Party" means any one of them;

1.5. **"Personal Information"** shall have the meaning ascribed to it in Chapter 1 of POPI;

1.6. **"POPI"** shall mean the Protection of Personal Information Act, No 4 of 2013, as amended from time to time, including any regulations and/or code of conduct made under the Act;

1.7. **"Privacy and Data Protection Conditions"** shall mean the 8 (eight) statutory prescribed conditions for the lawful Processing of Personal Information which is entered into a Record and such conditions are listed in Section 4(1) of POPI and are dealt with in detail in Part A of Chapter 3 of POPI;

1.8. **"Processing"** shall have the meaning ascribed to it in Chapter 1 of POPI;

1.9. **"Record"** shall have the meaning ascribed to it in Chapter 1 of POPI;

1.10. **"Responsible Party"** shall have the meaning ascribed to it in Chapter 1 of POPI; and

1.11. **"Signature Date"** means the date of last signature of this Agreement provided that it is signed by both of the Parties.

2. OPERATOR WARRANTY

2.1. The Operator warrants that when processing any Personal Information for and on behalf of RTT Group (Pty) Ltd it shall:

2.1.1. process such Personal Information only with the knowledge and authorisation of RTT Group (Pty) Ltd;

2.1.2. not disclose Personal Information to any third parties without the written consent of RTT Group (Pty) Ltd unless required by law or in the course of the proper performance of the Operator's duties;

2.1.3. have due regard to generally accepted information security practices and procedures which may apply to the Operator generally or be required in terms of specific industry or professional rules and regulations;

2.1.4. notify RTT Group (Pty) Ltd immediately where there are reasonable grounds to believe that Personal Information has been accessed or acquired by any unauthorised person;

2.1.5. establish and maintain security measures to 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 loss of, damage to, or unauthorised destruction of Personal Information and unlawful access to, or processing of, Personal Information and shall take reasonable measures to:

2.1.5.1. identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

2.1.5.2. establish and maintain appropriate safeguards against the risks identified;

2.1.5.3. regularly verify that the safeguards are effectively implemented; and

2.1.5.4. ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

3. PROTECTION OF PERSONAL INFORMATION

The Operator shall fully comply with the statutory obligations contained in POPI, with which the Operator warrants that it is fully conversant with as at the Signature Date, when Processing Personal Information obtained by the Operator from RTT Group (Pty) Ltd and when such Personal Information is entered into a Record. Without limiting the generality of the aforesaid the Operator shall ensure that the Privacy and Data Protection Conditions are strictly adhered to when Processing the Data Subject's Personal Information.

4. INDEMNITY

The Operator hereby indemnifies and holds RTT Group (Pty) Ltd harmless from any liability whatsoever arising from the Operator's failure to comply with the warranties contained in this Agreement and its statutory obligations contained in POPI.

ANNEXURE F– Employee Contract / Job Application Form Model Clauses

Protection of Personal information Act – Consent to Processing

I agree that personal information about me may be recorded, kept for as long as it required by the employer and processed by the employer for its legitimate interests, subject to the provisions of the Protection of Personal Information Act 4 of 2013.

Consent – Credit and Criminal Record

I hereby consent and authorise the employer or its duly authorized agent to make my name, surname, identity number and fingerprints available to the South African Police Service or any credit bureau and I hereby authorise the employer to conduct any credit references and/or to conduct criminal record enquiry as the employer in its sole discretion deems necessary.

I furthermore authorise the South African Police Service to furnish personal information regarding my criminal background, criminal history, previous convictions and/or any other relevant information such as usually furnished by the Criminal Record Centre of the South African Police Service in this regard, to the employer and/or the employer's duly authorised agent.

I furthermore unconditionally indemnify the South African Police Service and all its members, employees as well as the Government of the Republic of South Africa against any liability which results or may result from furnishing information in this regard.

I understand that it is a condition of the South African Police service, that-

a) The information is furnished solely for the purpose of my proposed employment/continuation of my employment with the employer;

b) any information furnished to the employer/the employer's duly authorised agent, will be disclosed to me for comments before a decision is made on my employment/application; and

c) employer/the employer's duly authorised agent is responsible for verifying the accuracy, in every respect, of the information furnished by the South African Police Service.

Consent – Employment References

I hereby consent and authorise the employer or its duly authorized agent to contact any of my references and to make enquiries in respect of my behaviour, work ethic, competence, expertise, work record, honesty and any related matters as the employer in its sole discretion deems necessary.

Consent – Qualification Verification

I hereby consent and authorise the employer or its duly authorized agent to verify any and all of my qualifications against any source as the employer in its sole discretion deems necessary.

Consent – Psychometric or Other Assessment Testing

I hereby consent and authorise the employer or its duly authorized agent to conduct any employment screening tests on me, including but not limited to, psychometric and other assessment tests, as the employer in its sole discretion deems necessary.

Consent – Third Party Processing and Further Processing

I hereby consent and authorise the employer or its duly authorized agent to share the information contained in this application form, or information related to the information in this application form, with third parties, where it is in the legitimate interests of the employer to do so, including but not limited to, other companies within RTT Group (Pty) Ltd and recruitment agencies and I hereby consent and authorise such third parties to process my personal information for reasons that are related to the legitimate interests of the employer or such third parties.

ANNEXURE G– Personal Information Sharing Policy

1. COMMITMENT

RTT Group (Pty) Ltd takes the protection of personal information seriously and aims to comply with POPI.

2. APPLICABILITY

2.1. This Personal Information Sharing Policy (the policy) applies to all staff working for RTT Group (Pty) Ltd which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. This policy is in addition to other requirements which may be necessary for specific operations and it is your responsibility to familiarise yourself with this policy.

2.2. "Personal information" means any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person. Personal information includes, for example, names and addresses, e-mail addresses, recruitment details, financial history and the like. It also includes opinions about individuals as well as facts and also applies to corporate contacts.

2.3. "Special personal information" is information such as religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.

3. OBLIGATIONS

3.1. Purpose definition and limitation

3.1.1. Personal information can only be collected and further processed for lawful, specific and explicitly defined purposes related to a function or activity of RTT Group (Pty) Ltd.

3.1.2. You will find an indication of such purposes in RTT Group (Pty) Ltd's Protection of Personal Information Policy and website privacy policy.

3.1.3. After personal information has been collected by RTT Group (Pty) Ltd it cannot be processed for purposes which are incompatible with the original ones.

3.1.4. For example, this means that personal information processed by the HR department for HR purposes will likely not be able to be lawfully processed by the marketing department for marketing purposes.

3.2. Personal information to be kept confidential

3.2.1. RTT Group (Pty) Ltd must keep personal information confidential and safe from undue disclosures.

3.2.2. That means that sharing personal information with an external third party is an exception to the confidentiality rule, and must be analysed in detail to ensure lawfulness, notably considering:

3.2.2.1. Whether the purpose for which the external third party requires the personal information is compatible to the original purpose for which the information was collected;

3.2.2.2. Whether sharing the personal information with the external third party will constitute a transborder flow of information; and

3.2.2.3. Whether sharing the personal information with the external third party will likely put the information at risk due to the poor security measures the third party has in place.

4. PROCEDURES TO FOLLOW

4.1. To assist you in dealing with a request to share personal information, we include flowchart procedures as Appendix B hereto.

4.2. If you receive a request for personal information you must:

4.2.1. Notify the IO who will guide you or, as the case may be, lead the procedures; and

4.2.2. Follow the flowcharts attached.

4.3. If you are required to share personal information, you must consider whether the personal information is to be shared internally (i.e. within RTT Group (Pty) Ltd) or externally (i.e. with an agent, a public authority, an unconnected third party or other entities within RTT Group (Pty) Ltd). When you are certain of the type of request you received, please check the flowcharts attached for guidance on the specific steps to take.

4.4. If you are unsure which category the personal information sharing falls into, please contact the IO for further advice.

4.5. You should document at all times any questions asked, answers given and authorisation gained by any parties involved when dealing with a personal information sharing request.

4.6. Where you are asked to share personal information with unconnected third parties / public authorities, the IO will handle the process himself/herself.

5. CLIENT INFORMATION

Personal information relating to clients should not be shared with third parties, including other entities within the RTT Group (Pty) Ltd without seeking further guidance from the IO.

6. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for RTT Group (Pty) Ltd and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

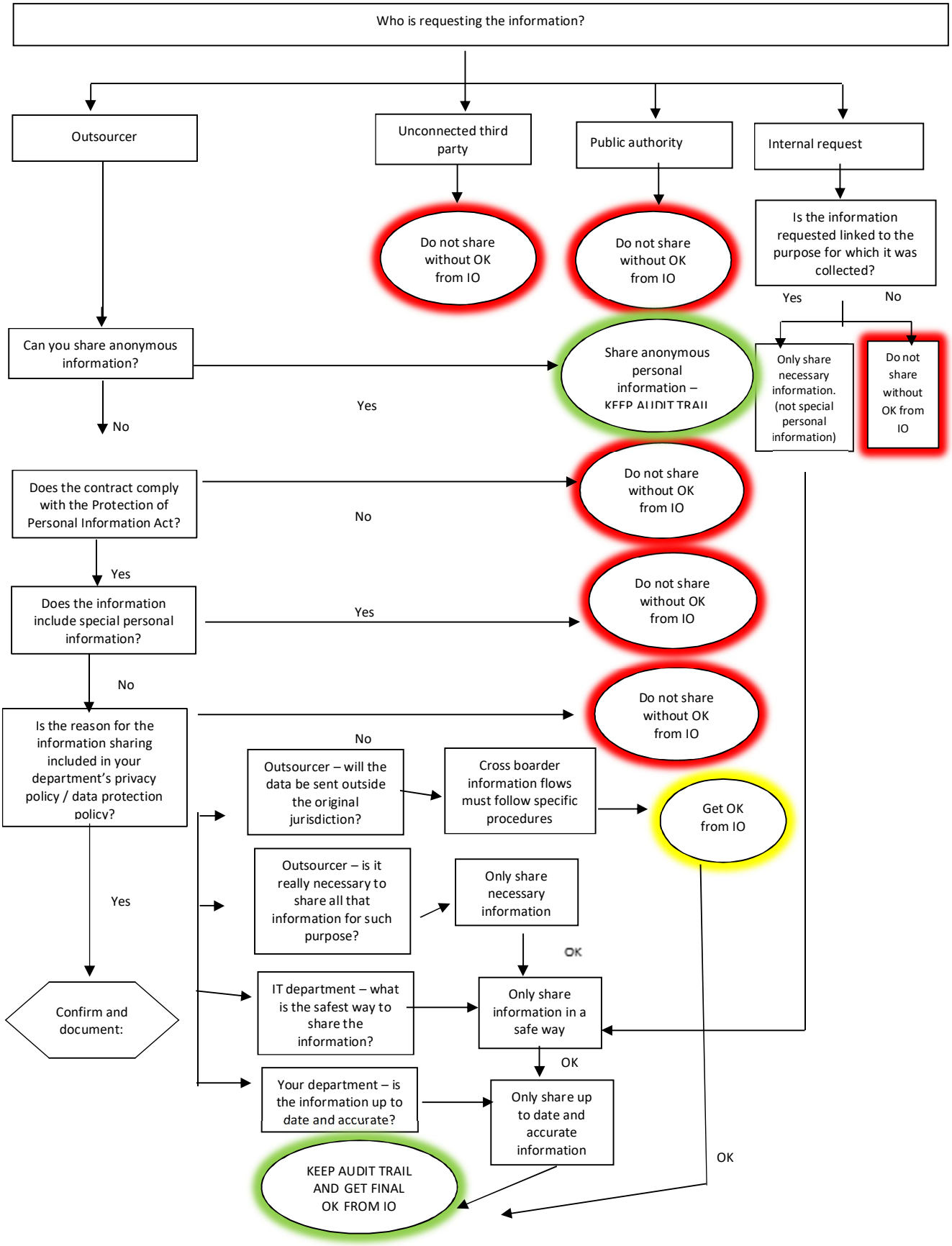
7. POLICY REVISION

This policy has been reviewed and approved by the IO and is subject to change without prior notice.

CONTACT DETAILS OF THE IO

Name: Anje Lubbe
Address: C/O SPRINGBOK & JONES ROAD BARTLETT BOKSBURG
E-mail address: Legal@rtt.co.za
Telephone number: 011 552 1000

Appendix B – Figure 1



ANNEXURE H – Subject Access Request Policy

1. INTRODUCTION

RTT Group (Pty) Ltd is required to comply with the requirements of POPI which gives data subjects the right to ask for a description of the personal information that RTT Group (Pty) Ltd holds about them.

2. APPLICATION AND CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

2.1. This policy applies to all staff of RTT Group (Pty) Ltd, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and RTT Group (Pty) Ltd reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. PURPOSE OF THIS DOCUMENT

3.1. This document outlines the process for dealing with Subject Access Requests that are received by RTT Group (Pty) Ltd and covers:

3.1.1. How to identify a Subject Access Request;

3.1.2. Who is entitled to make one ;

3.1.3. Who within RTT Group (Pty) Ltd is responsible for dealing with them;

3.1.4. The timescale for responding to one;

3.1.5. How to assess whether a Subject Access Request is valid;

3.1.6. How to set the scope of, and conduct any search for, information in response to a Subject Access Request;

3.1.7. What information should be provided in response to the Subject Access Request; and

3.1.8. What information may be withheld from a response to the Subject Access Request.

3.2. This document provides guidance only and in the event of a Subject Access Request please contact the IO immediately - please see the list at the end of the note for contact details of the IO.

4. RECEIPT OF SUBJECT ACCESS REQUESTS

4.1. A Subject Access Request may be received by RTT Group (Pty) Ltd in any of a number of different forms, including a telephone call, email or letter requesting access to personal information. Subject Access Requests generally tend to originate from current or past employees, job applicants, clients or third parties acting on their behalf (particularly where criminal or civil proceedings are involved).

4.2. In the first instance, it may not always be clear that a data subject is making a Subject Access Request. Therefore it is important to be familiar with this policy to be able to identify a Subject Access Request.

4.3. If you receive what you believe to be a Subject Access Request in any form then it is important that you forward a copy of the request to the IO immediately, who will manage the Subject Access Request.

4.4. In the case of a telephone call, it is best practice to inform the data subject that his/her/its request for information must be made in writing and cannot be processed otherwise. You should also notify the IO that the phone call has taken place.

4.5. Once you have passed the request on to the IO and have received an acknowledgement that it has been received, responsibility for processing the Subject Access Request will be managed by the IO and individuals from the relevant department within RTT Group (Pty) Ltd (as applicable).

5. TIME PERIOD FOR THE RESPONSE

5.1. RTT Group (Pty) Ltd must respond to a valid Subject Access Request within a reasonable period but always within 30 days.

5.2. Where a Subject Access Request is missing any of its required elements, it is essential that a prompt request for the missing part(s) is sent back to the data subject asking for the missing elements.

5.3. Once all of the requirements set out above have been met and the request has become a valid Subject Access Request, the stated period for providing a formal response must be complied with.

6. WHO IS ENTITLED TO MAKE A SUBJECT ACCESS REQUEST?

6.1. Any data subject is entitled to make a Subject Access Request to RTT Group (Pty) Ltd. RTT Group (Pty) Ltd will typically receive Subject Access Requests:

6.1.1. from its employees or former employees or job applicants;

6.1.2. from an individual working for a supplier or a supplier;

6.1.3. from a customer who is an individual or a customer; or

6.1.4. from an individual that has used RTT Group (Pty) Ltd's website.

6.2. These individuals and entities have a right to be informed by RTT Group (Pty) Ltd whether personal information about them is being processed. If personal data is being processed in almost any way by RTT Group (Pty) Ltd then the data subject is entitled to be given any of the following information:

6.2.1. a description of the personal information held; and

6.2.2. an indication of all the third parties or categories of third parties who have or have had of access to the information.

Validity of a Subject Access Request

6.3. It is necessary to confirm that the Subject Access Request is valid. The validity of a Subject Access Request will depend on the format and content of the Request. A valid Subject Access Request:

6.3.1. is in writing to RTT Group (Pty) Ltd's physical or postal address, fax number or e-mail address;

6.3.2. provides sufficient information to allow the identification of the individual requesting the personal information and the information requested;

6.3.3. indicates the form in which the information should be provided;

6.3.4. specifies an address, fax number or email address of the data subject in South Africa; and

6.3.5. includes sufficient identification of the individual to which the Subject Access Request relates.

7. IDENTIFICATION AND SEARCH TERMS

7.1. The IO must confirm the identity of the individual making the request - i.e. to confirm the person is who the person says it is.

7.2. Where the Subject Access Request is made by an employee or a former employee then this will normally be straightforward. The information to be requested will usually be the employee's/former employee's:

7.2.1. Employee ID;

7.2.2. Department;

7.2.3. Room or Desk number; and / or

7.2.4. Employee's telephone extension.

7.3. Where the Subject Access Request is made by someone other than an employee or a former employee then you should send a letter requesting confirmation of identity and also requesting, if necessary, further information to be provided to assist in focussing the search for information.

8. SETTING THE SCOPE AND CONDUCTING THE SEARCH

8.1. Subject Access Requests sometimes clearly identify specific information sought by the individual. This permits a simple and targeted search for that information.

8.2. However, other requests are expressed more widely and may, for example, simply request all information held about them (e.g "*Please send me a copy of all the information you have on me*"). Such a wide-ranging request would be difficult and onerous to comply with given the volume of information that would have to be reviewed.

8.3. When a wide-ranging request is made then the first step is always to contact the individual and try to obtain clarifications about the information that they actually want. This may often result in a much more specific request leading to a much more targeted search.

8.4. Typically, requests may focus on copies of interview notes, employment application forms, personnel files, appraisal information, holiday and leave information, CCTV footage and emails. However, if the individual is not prepared to focus their request then you should use the "Default RTT Group (Pty) Ltd Search Parameters" set out below.

8.5. In most cases:

8.5.1. the search should include any centrally held personnel files about the individual (such as RTT Group (Pty) Ltd's employee personnel file);

8.5.2. general and non-specific requests (e.g., for the provision of "all" information held about an individual) are not acceptable. The request must relate to specific personal information.

8.5.3. if the search relates to emails, then it should only apply to a limited number of email accounts over a limited period. Keyword searching may also be used; and

8.5.4. it is not necessary to restore back-up information in order to respond to the request unless the individual has a real need for specific information contained in the back-ups.

8.6. In general, when setting the parameters for a search, you must consider whether this constitutes a reasonable and proportionate search. This will generally depend on the circumstances but you should consider:

8.6.1. The likelihood that the information exists (i.e. is it just a “fishing expedition”?);

8.6.2. The value or importance of the information to the individual;

8.6.3. The cost of locating and reviewing the information; and

8.6.4. Whether the information is intended for use in litigation (while pending litigation doesn’t invalidate a Subject Access Request, it may be more appropriate for disclosure to be made during discovery).

9. THE DEFAULT SEARCH PARAMETERS

9.1. The Default Search Parameters attempt to take into account the above to provide a reasonable and proportionate response so searches for a general request for access to personal information should generally be based on the following parameters (noting that the specific facts on each request may dictate other search factors), however this may vary from request to request:

9.1.1. A copy of the data subject’s personnel file should be provided (in the case of an employee or a former employee);

9.1.2. Pre-defined keywords should be used to search email;

9.1.3. There should be no restoration of back up data without the prior approval of the IO.

9.2. It is important to note that any emails sent internally about the Subject Access Request itself will usually not need to be included in the response, on the basis that they may be legally privileged.

10. IT DEPARTMENT ASSISTANCE FOR ELECTRONIC RECORDS

10.1. The search may require the assistance of other departments, such as the IT department for tracking.

10.2. The IO should define a specific form to be used when requesting assistance from other department, which should set out clearly:

10.2.1. the names of the inbox owners;

10.2.2. the date range (no longer than [6 months] from the date that the valid Subject Access Request was received); and

10.2.3. relevant search terms and parameters.

11. WHICH INFORMATION THAT IS FOUND IN THE SEARCH MUST BE DISCLOSED AND WHAT CAN RTT Group (Pty) Ltd REFUSE TO DISCLOSE?

11.1. A Subject Access Request only entitles the individual to access personal information about himself/herself. In general, personal information about an individual is required to be disclosed if it identifies that individual.

11.2. However there are important exemptions which may apply. These exemptions apply to very specific information and are complex in its interpretation. The IO will analyse the retrieved personal information and shall apply any relevant exemption.

11.3. Such exemptions may, for example, include information:

11.3.1. That is subject to legal professional privilege; or

11.3.2. That reveals the identity of a third party individual.

12. OTHER INFORMATION TO BE INCLUDED IN THE RESPONSE

12.1. The individual is also entitled to information about the third parties or categories of third parties who have or have had access to his / her personal information.

13. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for RTT Group (Pty) Ltd and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

14. POLICY REVISION

This policy has been reviewed and approved by the IO and is subject to change without prior notice.

CONTACT DETAILS OF THE IO

Name: Anje Lubbe
Address: C/O SPRINGBOK & JONES ROAD BARTLETT BOKSBURG
E-mail address: Legal@rtt.co.za
Telephone number: 011 552 1000

ANNEXURE I– CCTV Monitoring Policy

1. ABOUT THIS POLICY

The purpose of this policy is to regulate the use of Closed-Circuit Television (CCTV) to monitor and record images for the purposes of safety and security.

2. APPLICATION AND CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

2.1. This policy applies to all staff of RTT Group (Pty) Ltd, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and RTT Group (Pty) Ltd reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. GENERAL PRINCIPLES

3.1. RTT Group (Pty) Ltd is committed to enhancing the quality of life of its employees by integrating the best practices with regard to workplace safety with the state of the art technology. A critical component of a comprehensive security program is the use of CCTV monitoring.

3.2. CCTV monitoring may be used in public areas by RTT Group (Pty) Ltd to deter crime and to assist in protecting employees and property.

3.3. Information obtained via CCTV monitoring will be used exclusively for security and law enforcement purposes. Information obtained by CCTV monitoring will only be released when so authorised by the IO.

3.4. CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with existing RTT Group (Pty) Ltd policies and practices and will be limited to uses that do not violate the reasonable expectation of privacy of data subjects.

3.5. Images and related data collected by CCTV are the property of RTT Group (Pty) Ltd.

4. RESPONSIBILITIES

4.1. The IO is responsible for authorizing all CCTV monitoring for safety and security purposes at RTT Group (Pty) Ltd and overseeing and coordinating the use of CCTV monitoring equipment at RTT Group (Pty) Ltd.

4.2. RTT Group (Pty) Ltd will monitor new developments in the law and industry standards in respect of CCTV monitoring.

5. PROCEDURES

5.1. RTT Group (Pty) Ltd will post signage where appropriate. An example of an appropriate sign is:

Images are being monitored and recorded for the purposes of crime prevention and public safety.

5.2. Individuals whose images are recorded have a right to view the images of themselves and to be provided with a copy of the images against the payment of a reasonable fee.

5.3. The CCTV systems used by RTT Group (Pty) Ltd will produce clear images which law enforcement bodies (such as the police) can use to investigate crime and that can easily be taken from the system when required.

5.4. CCTV cameras will be installed in positions where they can record clear images.

5.5. CCTV cameras will be positioned to avoid the capturing of images of persons not visiting the premises and residential housing. Any view given of housing will be no greater than what is available with unaided vision.

5.6. Images recorded by CCTV cameras will be securely stored and may only be accessed by authorised persons.

5.7. Images will not be provided to third parties other than law enforcement bodies.

5.8. Regular checks will be carried out to ensure that CCTV cameras are working properly and produce high-quality images.

5.9. CCTV monitoring will not be used in areas which workers would reasonably expect to be private, such as toilet areas and private offices.

5.10. The CCTV monitoring center will be configured so as to prevent the tampering with or duplicating of information.

5.11. Recorded images will be stored for a period not exceeding 14 days and will then be erased, unless retained as part of a criminal investigation or court proceedings or other legitimate use as approved by the IO.

6. CONSEQUENCES OF NON-COMPLIANCE

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for RTT Group (Pty) Ltd and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

7. POLICY REVISION

This policy has been reviewed and approved by the IO and is subject to change without prior notice.

CONTACT DETAILS OF THE IO

Name: Anje Lubbe
Address: C/O SPRINGBOK & JONES ROAD BARTLETT BOKSBURG
E-mail address: Legal@rtt.co.za
Telephone number: 011 552 1000

ANNEXURE J– Security Compromises Policy

1. OVERVIEW

1.1. Security compromises require centralised and swift management and this Security Compromises Policy (policy) outlines a framework for responding to such incidents.

1.2. It is essential for all staff to comply with this policy – Security compromises must be notified to the Regulator and to the affected individuals.

2. APPLICATION AND CONSEQUENCES OF NON-COMPLIANCE WITH THIS POLICY

2.1. This policy applies to all staff of RTT Group (Pty) Ltd, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and RTT Group (Pty) Ltd reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. KEY CONSIDERATIONS

3.1. RTT Group (Pty) Ltd has to comply with the Protection of Personal Information Act 4 of 2013 (POPI) to ensure that measures are taken to keep data secure, including specific legal obligations around dealing with a security compromise. Such legal requirements must be observed in addition to the approach set out in this policy.

3.2. This policy includes guidelines on how to deal with security compromises, including:

3.2.1. Containment and initial assessment;

3.2.2. Risk evaluation;

3.2.3. Breach notification;

3.2.4. Remedial action; and

3.2.5. Incident response plan.

4. CONTAINMENT AND INITIAL ASSESSMENT

4.1. An important starting point with any security compromise is to consider what steps are required in order to contain it. For example, if the incident involves a form of intrusion (via either internal or external threats) into RTT Group (Pty) Ltd's systems then containment action could include:

4.1.1. identification of where the intrusion itself is occurring on the systems;

4.1.2. closing down such weak points to contain the incident; and

4.1.3. prevention of further impact on data through the compromised systems.

4.2. **Team:** Using the risk classification outlined below, where the incident represents a risk that is categorised as a high or medium risk, then a security compromise management team should convene to address the incident.

4.3. **Team authority and scope:** The team should have appropriate representation from the IO and key departments such as, IT, information security, PR, legal, and should also have sufficient authority within RTT Group (Pty) Ltd to investigate and address the incident in accordance with this policy.

4.4. **Legal professional privilege:** Care should be taken to ensure that the investigation is carried out utilising to the maximum extent possible the protection of legal professional privilege. For example, engaging RTT Group (Pty) Ltd's legal team and/or appropriate external counsel from the outset may greatly assist in preserving legal professional privilege.

4.5. **Informing Stakeholders:** The investigation team should consider which other internal stakeholders should be informed of the incident and at what stage in the investigation process they should be informed.

4.6. **Confidentiality:** The investigation team should also consider keeping the investigation confidential from those (internally or externally) that do not need to be made aware of the investigation (either wholly or in part). This will allow the investigation to continue unhindered particularly with regard to further scoping of the incident and any activity around it. This may include, for example, notifying an appropriate law enforcement authority.

5. ASSESSING THE RISKS

5.1. The investigation team should assess the risks arising from the security compromise. The key driver behind identifying the risk is to assess and consider any potential adverse consequences, for example to:

5.1.1. individuals;

5.1.2. clients, or

5.1.3. employees.

5.2. These consequences should consider how serious or substantial the harm might be to anyone within these categories. The risk assessment will inevitably require a classification of the incident (see below) in order to drive the level of response required.

6. INCIDENT CLASSIFICATION

6.1. Incidents should be classified according to severity of risk, considering the following:

6.1.1. Level 1: High risk of:

6.1.1.1. harm to individuals whose confidentiality or data has been breached;

6.1.1.2. reputation damage to RTT Group (Pty) Ltd;

6.1.1.3. legal action from individuals or regulators.

6.1.2. Level 2: Medium risk of:

6.1.2.1. harm to individuals whose confidentiality or data has been breached;

6.1.2.2. reputation damage to RTT Group (Pty) Ltd;

6.1.2.3. legal action from individuals or regulators.

6.1.3. Level 3: Low risk of:

6.1.3.1. harm to individuals whose confidentiality or data has been breached;

6.1.3.2. reputation damage to RTT Group (Pty) Ltd;

All security compromises or suspected security compromises must be treated seriously.

Do not do anything to the suspected computer/s or other systems equipment, including turning on or off, or shut down the network unless instructed to do so by RTT Group (Pty) Ltd's Information Security team / Information Officer / legal team].

6.2. In practice the investigation may have a particular insight into the risk level from addressing the security compromise containment and the initial stages of the assessment (see above). However, this particular stage to evaluate the risk will require the investigation team to focus on determining factors such as the following (non-exhaustive):

6.2.1. What information:

6.2.1.1. was impacted by the security compromise (risk materialised therefore high risk); or

6.2.1.2. could have been subject to impact (risk could have materialised therefore medium risk) as a result of the security compromise?

6.2.2. Who is affected and what is the likelihood of any harm as a result of the incident?

6.2.3. Where was the information being processed and handled?

6.2.4. Which RTT Group (Pty) Ltd department / area / business / subsidiary / office is responsible for such processing and handling?

6.2.5. What was determined to be the cause of the security compromise?

6.2.6. What was determined to be the extent or reach of the security compromise?

6.3. **Regulatory reporting**: The investigation will require consideration of the reporting requirements under POPI and other South African ancillary rules. For that, the IO should be involved from the outset.

6.4. **Protective Measures**: Other factors of the investigation will focus around whether or not the personal information involved in the incident was subject to specific protective measures. For example:

6.4.1. Was encryption used?

6.4.2. What levels of encryption were used?

6.4.3. Was the encryption technology and the standard used sufficient to safeguard the individuals against any risks as a result of the breach incident?

6.5. As part of the investigation team's role they will need to establish exactly what information has been compromised and whether or not the incident took place within the control of RTT Group (Pty) Ltd or whether the risk materialised within the control of its third parties. In the case of third parties, the team will need to assess what obligations and responsibilities may flow under POPI and also the contract between RTT Group (Pty) Ltd and the third party.

7. NOTIFICATION OF SECURITY COMPROMISES

7.1. As a result of the investigations carried out during the evaluation of the risk (see above) RTT Group (Pty) Ltd may decide it is necessary to report the security compromise to third parties, which may include notifying the incident to:

7.1.1. The Regulator; or

7.1.2. Individuals whose personal information was accessed or acquired in the compromise (unless their identity cannot be established).

7.1.3. Other entities or organisations if required by specific legislation - for example, the South African Police Service, the National Intelligence Agency; and

7.1.4. Other entities or organisations, on an optional basis - for example customers, if deemed appropriate by the public relations department, senior management and the IO.

7.2. The team should consider seeking appropriate expert advice on the notification requirements.

7.3. The notification to the Regulator and the affected individuals must be made as soon as reasonably possible after the discovery of the compromise, taking into account the time it takes to spend on the initial containment, risk assessment and incident classification stages.

7.4. Notification to the affected individuals may only be delayed if the South African Police Service, the National Intelligence Agency or the Regulator determines that notification will harm a criminal investigation.

7.5. As such, the notifications to the South African Police Service, the National Intelligence Agency or the Regulator will have to be submitted before the affected individuals, and it must include a specific question on whether the notification to the affected individuals should be delayed.

7.6. The notification to the affected individuals must be in writing and communicated to the individual in at least one of the following ways:

7.6.1. mail;

7.6.2. e-mail;

7.6.3. placement on the website of RTT Group (Pty) Ltd;

7.6.4. publication in the news media; or

7.6.5. as may be directed by the Regulator.

7.7. The notification must provide sufficient information to allow the affected individuals to take protective measures against the potential consequences of the compromise. This may include, if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

8. EVALUATION AND RESPONSE

8.1. **Evaluation:** It is clearly essential for RTT Group (Pty) Ltd to conduct an appropriate investigation. RTT Group (Pty) Ltd must then analyse the risks arising from a security compromise and the effectiveness of the systems and controls within RTT Group (Pty) Ltd questioning why the particular weaknesses or failure points lead to the incident arising. For example, if the security compromise was caused entirely by or even in part attributed to a systemic problem within RTT Group (Pty) Ltd then simply containing the security compromise and then continuing on a "business as usual" approach would not be acceptable in the eyes of the Regulator.

8.2. **Response and implementation:** The investigatory team should ensure that the lessons learned from the incident should be incorporated into strengthening the existing controls and procedures around data management and security.

9. INCIDENT RESPONSE PLAN - CHECKLIST

9.1. RTT Group (Pty) Ltd should have, as an integral element of its security compromise response plan, a documented, methodical approach towards addressing the incident which should include factors such as the following:

9.2. **Evaluation of Risk – Assessing what actually happened:**

9.2.1. a determination of what information was involved;

9.2.2. to establish the cause of the incident and the extent of the security compromise;

9.2.3. determine who is actually affected by the security compromise;

9.2.4. consider the extent of which those affected by the security compromise will suffer any harm or otherwise assess the consequences as a result of the breach incident.

9.3. **Containment and initial Assessment:**

9.3.1. contain the security compromise;

9.3.2. assign responsibilities to investigate the incident;

9.3.3. assemble and authorise the investigation team;

9.3.4. notify defined internal stakeholders;

9.3.5. consider notification to any other third parties as may be required.

9.4. **Notification:**

9.4.1. allocate responsibilities;

9.4.2. seek expert assistance and advice;

9.4.3. notify the Regulator as soon as reasonably possible after discovering the compromise;

9.4.4. notify all affected individuals, if identifiable, unless told not to by the Regulator;

9.4.5. notify by methods such as: mail, email, press release or website publication;

9.4.6. include sufficient information in the notification to allow the affected individuals to take protective action against the potential consequences of the compromise.

9.5. **Remedial Action**

9.5.1. ensure that the risk register for RTT Group (Pty) Ltd is updated with all incidents and suspects incidents (near-misses);

9.5.2. update policies and procedures to ensure there will be measures to prevent of future breach incidents of this type;

9.5.3. review any issues raised around service delivery/third party partners;

9.5.4. test the revised incident and response plan;

9.5.5. finalise and implement the revise plan and conduct appropriate training.

10. CONSEQUENCES OF NON-COMPLIANCE

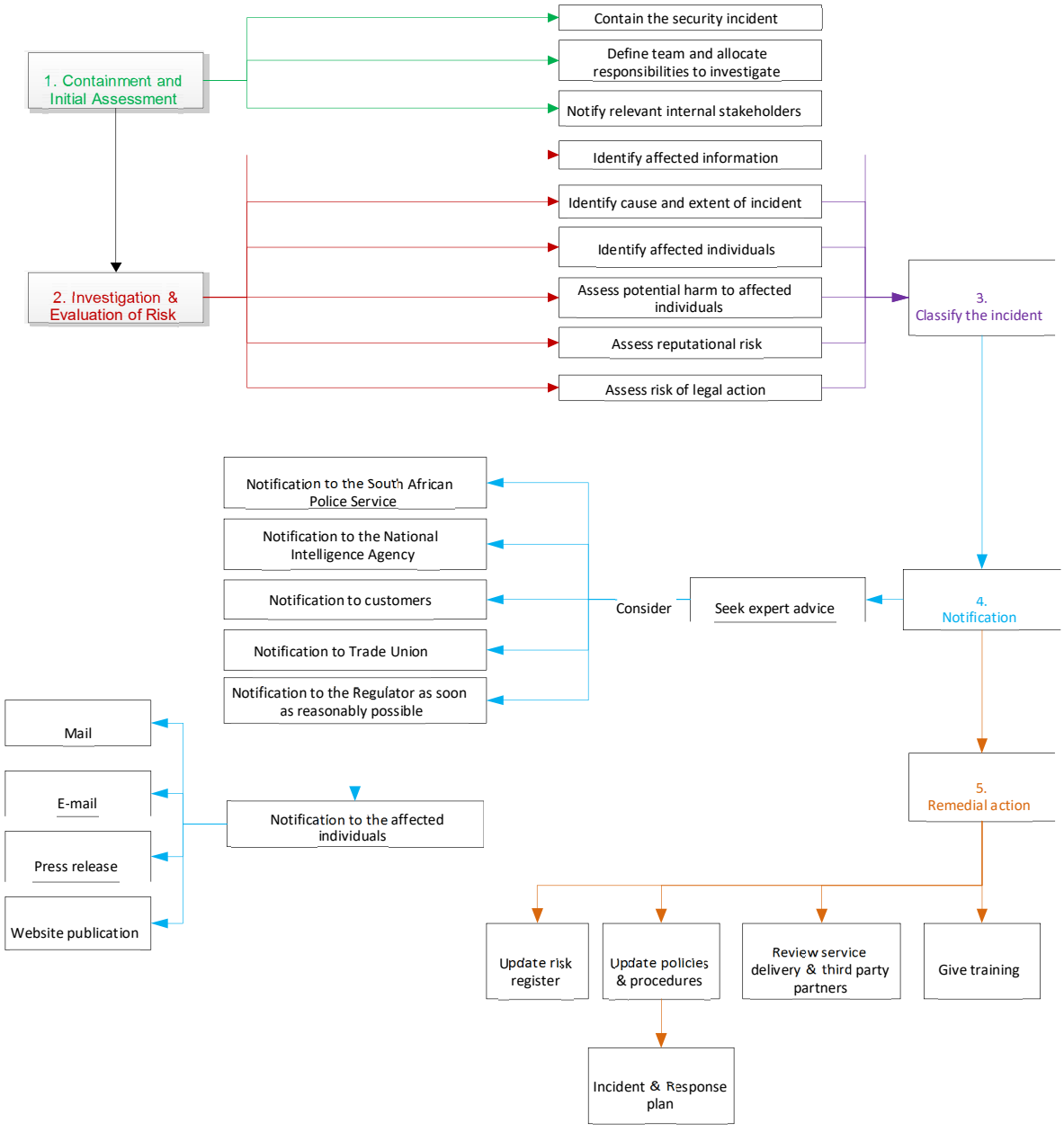
It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for RTT Group (Pty) Ltd and its employees. Failure to comply may lead to: disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

11. POLICY REVISION

This policy has been reviewed and approved by the IO and is subject to change without prior notice.

Security Compromises Procedure Flowchart

- Refer to the Policy for detailed guidelines
- Some steps may be taken contemporarily



ANNEXURE K – BYOD Policy

BRING YOUR OWN DEVICE POLICY

Portable storage devices, smartphones, tablets and certain media player technologies may provide the same functionality as laptops and personal computers and therefore pose an increased risk for RTT Group (Pty) Ltd in terms of keeping its network safe from malware.

While we grant our employees the privilege of using their own devices at work, we reserve the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of our data and technology infrastructure.

RTT Group (Pty) Ltd employees must agree to and abide by the terms and conditions of this policy if they wish to connect their own devices to our network.

12. Acceptable Use

12.1. Employees using their own devices are required to conform to the same security controls as outlined for personal computers or laptops.

12.2. Employees are blocked, at our sole discretion, from accessing certain websites during work hours or while connected to our network.

12.3. Devices may not be used at any time to:

12.3.1. store or transmit illegal materials;

12.3.2. store or transmit proprietary information belonging to RTT Group (Pty) Ltd or another company, other than allowed in terms of this policy; and

12.3.3. harass others;

12.4. Employees may use their mobile device to access the following company-owned resources:

12.4.1. Email and calendars; and

12.4.2. Contacts;

12.5. Where any device is used to connect to any company e-mail or file server, you must immediately report the loss, theft or damage of these devices to your direct manager, so that appropriate action can be taken to protect RTT Group (Pty) Ltd's information that may be on the device.

13. Devices and Support

13.1. Connectivity issues relating to RTT Group (Pty) Ltd's network are supported by IT. Employees should contact the device manufacturer or their carrier for operating system or hardware-related issues.

13.2. Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access our network.

14. Security

14.1. In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access our network.

14.2. The company's strong password policy applies.

14.3. The device must lock itself with a password or PIN if it's idle for five minutes.

14.4. After five failed login attempts, the device should lock.

14.5. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing our network.

14.6. Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.

14.7. Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to our network.

14.8. Employees' access to RTT Group (Pty) Ltd's data is limited based on user profiles defined by IT and automatically enforced.

14.9. Employees' device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of RTT Group (Pty) Ltd's data and technology infrastructure.

15. Risks/Liabilities/Disclaimers

15.1. While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up data.

15.2. We reserve the right to disconnect devices or disable services without notification.

15.3. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

15.4. Employees are expected to use his or her devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.

15.5. Employees are personally liable for all costs associated with his or her device.

15.6. Employees assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

15.7. We reserve the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

CONTACT DETAILS OF THE IO

Name: Anje Lubbe
Address: C/O SPRINGBOK & JONES ROAD BARTLETT BOKSBURG
E-mail address: Legal@rtt.co.za
Telephone number: 011 552 1000