MANUAL PREPARED IN TERMS OF SECTION 51

OF THE

PROMOTION OF ACCESS TO INFORMATION

ACT 2 OF 2000

Reckitt Benckiser South Africa (Proprietary) Limited &

Reckitt Benckiser Pharmaceuticals (Proprietary) Limited

CONTENTS	
1.	Introduction
2.	Contact details
3.	Section 10 Guide on how to use the Act
4.	Records available in terms of any other legislation
5.	Categories of records which are available without request
6.	Description of the subjects on which the Company holds records and the categories of records held on each subject
7.	Request procedure in terms of the Act
8.	Fees payable
9.	Other information as prescribed
10.	Processing of Personal Information
11.	Annexures

1. INTRODUCTION

1.1. Reckitt Benckiser Pharmaceuticals (Proprietary) Limited ("the Company"), is a Company incorporated in the Republic of South Africa and forms part of the Group of Companies in the Reckitt Benckiser Group ("Reckitt Group"), and continue to be engaged in the manufacture, marketing and distribution of a range of high-quality health, pharmaceutical, hygiene and household products.

1.2. This Manual has been compiled in accordance with the requirements of the Promotion of Access to Information Act, Act No. 2 of 2000 ("**the Act**"). The Company is a private body as defined in the Act, and this Manual contains the information specified in section 51(1) of the Act, which is applicable to such private bodies. This information is as follows:

1.2.1. the contact details of the head of the private body;

1.2.2. a description of the guide referred to in section 10 of the Act;

1.2.3. the latest notice published by the Minister under section 52(2) of the Act;

1.2.4. a description of the records of the private body which are available in terms of any legislation other than the Act;

1.2.5. a description of the subjects on which each private body holds records and the categories of records held on each subject in sufficient detail to facilitate a request for access to a record; and

1.2.6. other information as prescribed by regulation.

1.3. The Manual will be updated on a regular basis in accordance with the requirements of section 51(2) of the Act.

1.4. In this Manual, the following words bear the meaning set out below:

1.4.1 "**BEE**"	means black economic empowerment;
1.4.2 "**Client**"	means a natural or juristic person who or which receives services from the Company;
1.4.3 "**Company"**	means Reckitt Benckiser Pharmaceuticals (Proprietary) Limited with registration number 1943/016101/07 a company incorporated in accordance with the laws of the Republic of South Africa;

1.4.4 "**Employee**"	means any person who works for or provides services to or on behalf of the Company, and receives or is entitled to receive remuneration;
1.4.5 **"Guide"**	means the guide published by the SAHRC in terms of section 10 of the Act;
1.4.6 "**the/this Manual**"	means this Manual which is published in accordance with section 51 of the Act and "this Manual" shall have the same meaning;
1.4.7 "**the Minister"**	means the Cabinet member responsible for the administration of justice, presently the Minister of Justice and Constitutional Development;
1.4.8 "**Personal Information**"	means the information of a data subject as defined in the Protection of Personal Information Act, 2013, section 1: 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable existing juristic person, including, but not limited to—

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

1.4.8.2 information relating to the education or the medical, financial, criminal or employment history of the person;

1.4.8.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

1.4.8.4 the biometric information of the person;

1.4.8.5 the personal opinions, views or preferences of the person;

1.4.8.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

1.4.8.7 the views or opinions of another individual about the person; and

1.4.8.8 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;

1.4.9 "**POPIA**" means the Protection of Personal Information Act 4 of 2013;

1.4.10 "**Requester**" means any person or entity requesting access to a record that is under the control of the Company;

1.4.11 "**SAHRC**" means the South African Human Rights Commission;

1.4.12 "**the Act**" means Promotion of Access to Information Act. 2 of 2000 (as amended);

1.4.13 "**Head of the Company**" means the General Manager/s of the Company, or any person duly authorised by him or her to carry out the duties ascribed to the "head" of a private body by the Act.;

2. CONTACT DETAILS

2.1. The Head of the Company as mentioned below, is the head of the Company for the purposes of the Act and is the person to whom requests for access to records should be addressed.

2.1.1. Reckitt Benckiser Pharmaceuticals (Pty) Ltd

2.1.1.1. Name of General Manager: Ioannis Ntostas

2.1.1.2. Physical address of the Company: Ground Floor, North Wing, Allandale Building, 39 Magwa Crescent, Waterfall, 2090

2.1.1.3. Postal address of the Company: P.O. Box 164, Isando, 1600

2.1.1.4. Telephone of the Company: +27 11 871 1611

2.1.1.5. E-mail address of the head of the Company: Ioannis.Dostas@reckitt.com

3. SECTION 10 GUIDE ON HOW TO USE THE ACT

3.1. The SAHRC has, in terms of section 10 of the Act, published a Guide to assist persons wishing to exercise any rights in terms of the Act.

3.2. The Guide may be obtained from the SAHRC. Any person wishing to obtain the Guide may either access it through the website of the SAHRC at www.sahrc.org.za or should contact:

3.2.1. PAIA Unit

Research and Documentation Department

South African Human Rights Commission

Private Bag X2700, Houghton, 2041

Telephone: (011) 877 3600

Fax: (011) 403 0625 & Email: PAIA@sahrc.org.za

4. RECORDS AVAILABLE IN TERMS OF ANY OTHER LEGISLATION

4.1. Certain records held by the Company are available in terms of legislation other than the Act.

4.2. The specific records which are available in terms of such legislation are set out therein and

these records may in certain instances only be accessed by the persons specified in the relevant legislation. The legislation is as follows:

4.2.1. Basic Conditions of Employment Act, Act No. 75 of 1997;
4.2.2. Companies Act, Act No. 71 of 2008;
4.2.3. Compensation for Occupational Injuries and Diseases Act, Act No. 130 of 1993;
4.2.4. Competition Act, Act No. 89 of 1998;
4.2.5. Consumer Protection Act, Act No. 68 of 2008;
4.2.6. Employment Equity Act, Act No. 55 of 1998;
4.2.7. Fertilizers, Farm Feeds, Seeds and Remedies Act, Act No. 36 of 1947;
4.2.8. Foods, Cosmetics and Disinfectants Act, Act No. 54 of 1972;
4.2.9. Income Tax Act, Act No. 58 of 1962;
4.2.10. Labour Relations Act, Act No. 66 of 1995;
4.2.11. Legal Metrology Act, Act No. 9 of 2014;
4.2.12. Measurement Units and Measurement Standards Act, Act No. 18 of 2006;
4.2.13. Medical Schemes Act, Act No. 131 of 1998;
4.2.14. National Consumer Act, Act No. 34 of 2005;
4.2.15. National Regulator for Compulsory Specifications Act, Act No. 5 of 2008;
4.2.16. Occupational Health and Safety Act, Act No. 85 of 1993;
4.2.17. Pension Funds Act, Act No. 24 of 1956;
4.2.18. Protection of Personal Information Act, Act No. 4 of 2013;
4.2.19. Skills Development Act, Act No. 97 of 1998;
4.2.20. Skills Development Levies Act, Act No. 9 of 1999;
4.2.21. Unemployment Insurance Act, Act No. 63 of 2001;
4.2.22. Unemployment Insurance Contributions Act, Act No. 4 of 2002;
4.2.23. Value Added Tax Act, Act No. 89 of 1991.

5. CATEGORIES OF RECORDS WHICH ARE AVAILABLE WITHOUT REQUEST

5.1. No notices relating to the Company have been published by the Minister in terms of section 52(2) of the Act.

5.2. Certain records are available without needing to be requested in terms of the request procedures set out in the Act and detailed in Section 7 of this manual. This information may be inspected, collected, purchased or copied (at the prescribed fee for reproduction) at the offices of the Company. Certain information is also available on the Company's website www.rb.com. The records include:

5.2.1. Marketing brochures;

5.2.2. Company and Product websites;

5.2.3. Product content on Social Media;

5.2.4. Product Information;

5.2.5. Usage Instructions.

6. DESCRIPTION OF THE SUBJECTS ON WHICH THE COMPANIES HOLD RECORDS AND THE CATEGORIES OF RECORDS HELD ON EACH SUBJECT

6.1. The following is a list of the subjects on which the Company hold records and the categories into which such records fall. The procedure in terms of which such records may be requested from the Company is set out in Section 7 of this Manual. The records listed below will not in all instances be provided to a requester who requests them in terms of the Act. The requester should show that he or she has the right in terms of the Act to be given access to the records in question.

6.2. Categories of Records and Description of Records held-

6.2.1. Administration, Secretarial and Legal:

6.2.1.1. Shareholder records;

6.2.1.2. Share register;

6.2.1.3. Minutes of meetings of directors;

6.2.1.4. Records relating to the incorporation of the Company;

6.2.1.5. Minutes of meetings of committees and sub-committees;

6.2.1.6. Power of Attorney;

6.2.1.7. Record of major litigation/arbitration proceedings;

6.2.1.8. Insurance policies;

6.2.1.9. Title deeds;

6.2.1.10. Mortgage bonds;

6.2.1.11. Trademark, copyright, patent, service mark certificates and registrations.

6.2.2. Management:

6.2.2.1. Minutes of meetings of Executive Committee;

6.2.2.2. Internal correspondence;

6.2.2.3. Resolutions of the directors of the Company.

6.2.3. Finance:

6.2.3.1. Accounting records;

6.2.3.2. Tax records;

6.2.3.3. Debtors' records;

6.2.3.4. Creditors' records;

6.2.3.5. Insurance records;

6.2.3.6. Auditors' reports;

6.2.3.7. Interim and annual financial statements;

6.2.3.8. Bank statements and other banking records for business and trust accounts;

6.2.3.9. Invoices issued in respect of debtors and billing information;

6.2.3.10. Records regarding the Company's financial commitments.

6.2.4. Human Resources:

6.2.4.1. List of employees;

6.2.4.2. Statistics regarding employees;

6.2.4.3. Employment contracts;

6.2.4.4. Conditions of employment;

6.2.4.5. Information relating to prospective employees;

6.2.4.6. Personnel records including personal details, disciplinary records, performance and internal evaluation records;

6.2.4.7. CCMA records;

6.2.4.8. Registrations with Department of Labour: UIF, COIDA and Skills Development Levies Act;

6.2.4.9. Employee tax information;

6.2.4.10. Records of Unemployment Insurance Fund contributions;

6.2.4.11. Records regarding group life assurance and disability income protection;

6.2.4.12. Provide fund records;

6.2.4.13. Payroll records;

6.2.4.14. Health and safety records;

6.2.4.15. Workplace skills plans;

6.2.4.16. Codes of conduct;

6.2.4.17. Disciplinary code and procedure;

6.2.4.18. Grievance procedure;

6.2.4.19. Appeal procedure;

6.2.4.20. Remuneration policy;

6.2.4.21. Training schedules and material.

6.2.4.22. Internal policies and procedures regarding dismissals, performance appraisal, recruitment, selection, advertising of positions, appointments, retirement promotions, leave, extended sick leave, study leave, salaries, overtime, bonuses, medical aid, health and safety, adoption leave and benefits, BEE procurement, loans, working parents, black economic empowerment, smoking, use of company resources including telephones, motor vehicles and computers, sexual harassment, HIV-Aids and Pro Bono policy;

6.2.4.23. Correspondence relating to personnel.

6.2.5. Supplier

6.2.5.1. Supplier lists and details of suppliers;

6.2.5.2. Agreements with suppliers.

6.2.6. Information Technology Department

6.2.6.1. Computer software;

6.2.6.2. Support and maintenance agreements;

6.2.6.3. Records regarding computer systems and programmes;

6.2.6.4. User Manuals and licenses

6.2.7. Property

6.2.7.1. Asset registers;

6.2.7.2. Lease agreements in respect of immovable property;

6.2.7.3. Records regarding insurance in respect of movable property;

6.2.7.4. Records regarding insurance in respect of immovable property

6.2.8. Procurement

6.2.8.1. Records of tenders and vendor applications;

6.2.8.2. Policy and procedure of tenders

6.2.9. Supply Services

6.2.9.1. Supply services lists with freight providers and details of freight haulers;

6.2.9.2. Agreements with Freight Haulers;

6.2.9.3. Claim process records;

6.2.9.4. Records of delivery and dispatch of company products.

6.2.10. Marketing Department

6.2.10.1. Marketing, advertising and promotional material of products.

6.2.11. Research and Development

6.2.11.1. Records of various laboratory tests, reports, research and development material on household and pharmaceutical products.

6.2.12. Sales Department

6.2.12.1. Records of agreements, invoices, rebate structures and pricing with customers and distributors;

6.2.12.2. Credit Applications;

6.2.12.3. Customer and Distributor details.

6.2.13. Safety, Health and Environment

6.2.13.1. Complete Safety, Health and Environment Risk Assessment;

6.2.13.2. Environmental Managements Plans;

6.2.13.3. Inquiries, inspections, examinations by environmental authorities.

6.2.14. Corporate Affairs

6.2.14.1. Records of all donations to education and society.

6.2.15. Miscellaneous

6.2.15.1. Internal correspondence;

6.2.15.2. Firm publications.

7. REQUEST PROCEDURE IN TERMS OF THE ACT

7.1. A request for access to records held by the Companyin terms of section 50 of the Act must be made on the form contained in the Regulations Regarding the Promotion of Access to Information (Form C). A copy of the form is attached as Annexure A to this manual. The request must be made to the Companyat the address, or email address, specified in Section 2 above.

7.2. A requester must provide sufficient detail on the prescribed form to allow the Company to identify the record or records which have been requested and the identity of the requester. If a request is made on behalf of another person or entity, the requester must submit details and proof of the capacity in which the requester is making the request, which must be reasonably satisfactory to the Company. The requester is also required to indicate the form of access to the relevant records that is required, and to provide his, her or its contact details in the Republic of South Africa.

7.3. The requester must identify the right that he, she or it is seeking to exercise by accessing records held by the Company and must explain why the particular record or records requested is or are required for the exercise or protection of that right.

7.4. The Company may, and must in certain instances, refuse access to records on any of the grounds set out in Chapter 4 of Part 3 of the Act which include: that access would result in the unreasonable disclosure of personal information about a third party, that it is necessary to protect the commercial information of a third party or the Companyitself, that it is necessary to protect the confidential information of a third party, that it is necessary to protect the safety of individuals or property, that a record constitutes privileged information for the purpose of legal proceedings, and that it is necessary to protect the research information of a third party or the Company itself. Access to documents may also be refused on the basis of professional privilege.

7.5. The Companyis required to inform a requester in writing of its decision in relation to a request. If the requester wishes to be informed of the Company's decision in another manner as well, this must be set out in the request and the relevant details included, to allow the Company to inform the requester in the preferred manner.

7.6. The Companywill make a decision in relation to a request for records within 30 days of receiving it, unless third parties are required to be notified of the request or the 30-day period is extended as provided for in the Act. The Company/(ies) will notify the requester if the 30- day period for processing a request is to be extended.

7.7. Where a request is refused, a requester may apply to the High Court within 30 days of being informed of the refusal of the request, for an order compelling the record or records requested to be made available to the requester or for another appropriate order. The Court will determine whether the records should be made available or not. Notwithstanding the above, a requester may lodge a complaint to the Information Regulator (the complaint must be made in writing), against the access fee to be paid or the form of access granted, as referred to in terms of section 63(3) and 74(2) – the format of the complaint is available on the Information Regulator's website and can also be requested from the Company directly. The Information Regulator is required to give reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Information Regulator, to put the complaint in writing.

8. FEES PAYABLE

8.1. A requester has to pay a request fee of R50.00, other than where the requester is seeking access to a record containing personal information about him, her, their or itself. The requester may lodge a complaint to the Information Regulator as described above, against the access fee to be paid or the form of access granted. If the requester is seeking reproduction of a record containing personal information, then a fee may be charged. This request fee may be paid at the time a request is made, or the person authorised to deal with such requests on the Company's/(ies)' behalf may notify the requester that he, she, them or it needs to pay the request fee before processing the request any further. A requester may apply to Court to be exempted from the requirement to pay the request fee.

8.2. Where a request for access to a record or records held by the Company/(ies) is granted, the requester also has to pay an access fee for the reproduction of the record or records, and for the search for and the preparation of the records for disclosure. The Company/(ies) is entitled to withhold a record until the required access fees have been paid. The access fees which are payable are as follows:

8.2.2. Action taken Fee

8.2.1.1. Photocopy of an A4-size page or part thereof	R1.10
8.2.1.2. Printed of an A4-size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
8.2.1.3. For a copy in a computer-readable form on –	
stiffy disc	R7.50
compact disc	R70.00
8.2.1.4. Transcription of visual images, for an A4-size page or part thereof	R40.00
8.2.1.5. Copy of visual images	R60.00
8.2.1.6. Transcription of an audio record, for an A4-size page or part thereof	R20.00
8.2.1.7. Copy of an audio record	R30.00

8.3. In addition, if the search for and preparation of the record or records requested takes more than six hours, the Company/(ies) may charge R30.00 for each hour or part thereof which is required for the search for and preparation of the records.

8.4. If the Company/(ies) is of the opinion that the search for and the preparation of the records requested will require more than six hours, the Company/(ies) is entitled to ask for a deposit of one third of the access fees which will be payable in respect of the records requested by the requester. The requester may make an application to Court to be exempted from the requirement to pay this deposit. If a deposit is made and access to the records requested is subsequently refused, the deposit will be repaid to the requester.

9. OTHER INFORMATION AS PRESCRIBED

9.1. The Minister has not prescribed that any further information must be contained in this manual.

10. PROCESSING OF PERSONAL INFORMATION

10.1. The purposes for which the Company process or will process Personal Information is to allow the

Company to ensure that it best aligns the consumer's needs with the services available, or otherwise as is provided for under lawful processing in the Act.

10.2. Purpose of the Processing of Personal Information

10.2.1. HR

10.2.1.1. To enable the RB Group to maintain appropriate human resources records in relation to members of staff, including recruitment and selection, administration of payroll, expenses, accounts, tax, travel and benefits, work management, professional development and performance reviews, discipline and superannuation.

10.2.1.2. To enable Reckitt Benckiser Group to operate a workplace whistleblowing hotline to detect and prevent improper workplace conduct and crime prevention in accordance with relevant business conduct policies.

10.2.2. Customer Marketing

10.2.2.1. To enable the RB Group to maintain a customer relationship marketing database of individuals to whom information and promotional material may be sent in relation to products and services that may be of interest to them.

10.2.3. Customer Care

10.2.3.1. To enable consumer care via call centres to be provided including integrating external and internal management consumer information across the Reckitt Group, embracing finance, manufacturing, sales and procurement.

10.2.4. IT Administration

10.2.4.1. To enable IT administration to manage users of the Reckitt Group's network, allowing staff secure access to their IT systems, backing up information on the Company's network, document management, email system (Microsoft Exchange) and intranet service (RBOnline).

10.2.5. Accounts and Records Procurement

10.2.5.1. To enable procurement of goods and services by Reckitt Group.

10.2.6. Crime Prevention and Prosecution of Offenders

10.2.6.1. To enable the prevention and detection of a crime or alleged crime through the use of CCTV on Reckitt Group sites.

10.3. Categories of Data Subjects and Personal Information/special Personal Information relating thereto. As per section 1 of POPIA, a data subject may either be a natural or a juristic person.

10.3.1. HR

The personal data will include:

10.3.1.1. names and contact details of the data subject;

10.3.1.2. employment details;

10.3.1.3. financial details;

10.3.1.4. educational experience, business activities and skill set;

10.3.1.5. family members (where provided as point of contact); in Mexico

10.3.1.6. social activities, hobbies (as cultural, sports, professional, civic), family information

10.3.2. Customer Marketing

The personal data will include:

10.3.2.1. names and contact details of the data subject including email and telephone details;

10.3.2.2. country of residence;

10.3.2.3. nationality;

10.3.2.4. goods or services provided.

10.3.3. Customer Care

The personal data will include

- names and contact details of the data subject;
- (ii) employment details;
- (iii) financial details; (iv) educational experience, business activities and skill set;
- (v) family members (where provided as point of contact);
- (vi) goods or services provided.

10.2.1 IT Administration

The personal data will include

- names and contact details of the data subject;
- employment details;
- (iii) family members (where provided as point of contact).

10.2.2 Accounts and Records Procurement

The personal data will include

- names and contact details of the data subject;
- employment details;
- goods or services provided

10.2.3 Crime Prevention and Prosecution of Offenders

- The personal data will include images of the data subject.

10.2. Recipients or categories of recipients of Personal Information to whom Personal Information may be supplied

10.3.1. The Company may provide a data subject's Personal Information to recipients to which disclosure is required for regulatory compliance or otherwise as provided for within the provisions of the act, with reference to "processing'':

'Section 1: "processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

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

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

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;"

10.3.2. The Company will not without grounds for lawful processing, disclose personal information of the data subject in contravention of the data subject's right to privacy.

10.3. Planned Transborder flow of Personal Information

10.4.1. The following is a list of the planned cross-border transfers of Personal Information is as set out in the Intra Group Transfer agreement

10.4. The Reckitt Group is committed to safeguarding the security of all personal data which it processes through day-to-day operations. To achieve this, the Reckitt Group has developed and implemented technical and organisational measures that strive to safeguard this important asset. The measures form a robust Information Security protection program made up of data

privacy and security policies and functional specific Standard Operating Procedures, which include the following measures:

10.5.1 Information Security Policies and Standards:

10.5.1.1 Reckitt will implement security requirements within the organisation and for staff and all Sub processors, service providers, or agents who have access to Personal Data to maintain the integrity, confidentiality, resilience and availability of Personal Data, to include (but not be limited to) the following:

- Prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);
- Prevent Personal Data processing systems being used without authorization (logical access control);
- Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);
- Ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified, with appropriate pseudonymization and encryption measures adopted to protect the confidentiality of data during transfer and storage (data transfer and storage control);
- Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing (entry control);
- Ensure that Personal Data are Processed solely in accordance with transferor / data exporter's Instructions (control of instructions);
- Ensure that Personal Data are protected against accidental

destruction or loss, and appropriate measures adopted to support access to data and / or restoration of data in the event of a physical or technical incident impacting availability (availability control); and

- Ensure that Personal Data collected for different purposes can be processed separately (separation control).

10.5.1.2 These rules shall be kept up to date and revised whenever relevant changes are made to any information system that uses or houses Personal Data, or to how that system is organised.

10.5.1.3 These rules shall be routinely reviewed to evaluate efficacy and areas for improvement and where relevant adopt and apply changes as part of a continuous improvement programme.

10.5.2 Physical Security

10.5.2.1 The transferee / data importer will maintain commercially reasonable security systems at all transferee / data importer sites at which an information system that uses or houses Personal Data is located. The Suppler reasonably and appropriately restrict access to such Personal Data.

10.5.2.2 Physical access control shall be implemented for all data centres. unauthorised access is prohibited through 24x7 onsite staff and security camera monitoring.

10.5.3 Organisational Security

10.5.3.1 The transferee / data importer shall ensure that it has implemented security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

10.5.3.2 All Personal Data security incidents shall be managed in accordance with appropriate incident response procedures.

10.5.4. Network Security

10.5.4.1 The transferee / data importer shall maintain network security using

commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, access control lists and routing protocols.

10.5.5 Access Control

10.5.5.1. Only authorised staff shall be permitted to grant, modify or revoke access to an information system that uses or houses Personal Data.

10.5.5.2. User administration procedures shall be adopted which define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

10.5.5.3. All employees of the transferee / data importer shall be assigned unique User-IDs.

10.5.5.4. Access rights shall be implemented adhering to the “least privilege” approach.

10.5.5.5. The transferee / data importer shall implement commercially reasonable physical and electronic security to create and protect passwords.

10.5.5.6. Virus and Malware Controls

- The transferee / data importer shall install and maintain industry standard (which shall comprise the latest version) anti-virus and malware protection software on the system.

10.5.6. Personnel

10.5.6.1 The transferee / data importer shall implement a security awareness program to train personnel about their security obligations. This program shall include training about data classification obligations, physical security controls, security practices and security incident reporting.

10.5.6.2 The transferee / data importer shall have clearly defined roles and responsibilities for its employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.

10.5.6.3. The transferee / data importer personnel shall strictly follow established security policies and procedures. Disciplinary process will be appropriately

applied if employees commit a security breach.

10.5.7 Additional Security Requirements

10.5.7.1 The transferee / data importer shall not delete or remove any proprietary notices contained within or relating to Personal Data.

10.5.7.2 The transferee / data importer shall perform and maintain secure back-ups of all Personal Data and shall ensure that up-to-date back-ups are stored off- site. transferee / data importer shall ensure that such back-ups are available to transferor / data exporter (or to such other person as transferor / data exporter may direct) at no additional cost to transferor / data exporter, and that the data contained in the back-ups are available at all times upon request and are delivered to transferor / data exporter at no less than six (6) monthly intervals (or such other intervals as may be agreed in writing between the Parties).

10.5.7.3 The transferee / data importer shall ensure that any system on which it holds any Personal Data, including back-up data, is a secure system that complies with all security requirements.

10.5.7.4. If Personal Data is corrupted, lost or sufficiently degraded as a result of the transferee / data importer 's default so as to be unusable, transferor / data exporter may:

- require the transferee / data importer (at the transferee / data importer ’s expense) to restore or procure the restoration of Personal Data to the extent possible and transferee /

data importer shall do so as soon as practicable but not later than five (5) days from the date of receipt of transferor / data exporter's notice; and/or

- itself restore or procure the restoration of Personal Data and shall be repaid by the transferee / data importer any reasonable expenses incurred in doing so.

10.5.7.5 If at any time the transferee / data importer suspects or has reason to believe that Personal Data has or may become corrupted, lost or sufficiently degraded in any way for any reason, then the transferee / data importer shall notify transferor / data exporter immediately and inform transferor / data exporter of the remedial action the transferee / data importer proposes to take.

10.5.8 Malicious Software

10.5.8.1 The transferee / data importer shall, as an enduring obligation and at no cost to transferor / data exporter, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the relevant IT environment (or as otherwise agreed by the Parties).

10.5.8.2 The transferee / data importer may be required to provide details of the version of anti-virus software being used in certain circumstances (e.g. in response to a specific threat).

10.5.8.3 Notwithstanding the above, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Personal Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

10.5.8.4 Any cost arising out of the actions of the Parties taken in compliance with the above provisions shall be borne by the Parties as follows:

- by the transferee / data importer where the Malicious Software originates from the transferee / data importer 's software, the third- party software

supplied by the transferee / data importer (except where transferor / data exporter has waived the obligation) or Personal Data (whilst such Personal Data was under the control of the transferee / data importer or any of its Sub processors) unless the transferee / data importer can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by transferor / data exporter when provided to the transferee / data importer ; and

- Otherwise by transferor / data exporter

11. Annexure A: J752 PAIA Form C

J752 PAIA Form C

J752_paia_Form C.pdf