

# PROTECTION OF PERSONAL INFORMATION POLICY / POPIA POLICY

POLICY NUMBER

REVISION NUMBER

1

PAGE NUMBER

EFFECTIVE DATE

1

22 July 2021

## PROTECTION OF PERSONAL INFORMATION POLICY

### BACKGROUND TO DATA PRIVACY IN SOUTH AFRICA

The Protection of Personal Information Act, 4 of 2013, (“**POPIA**”), which came into force on 1 July 2021, is a statute that regulates the use and processing of a person and/or legal entity’s personal information, in order to protect and give effect to a person and/or legal entity’s rights to privacy, including the right not to have their personal information misused, abused or used for ulterior purposes.

POPIA applies to personal information that is the property of individuals and legal entities (“**Data Subjects**”) that is processed, be it in an automated or non-automated manner in South Africa, by another (“**Responsible Party**”) and places a duty to use it lawfully and only for a specific and defined purpose(s) on any Responsible Party who is processing a Data Subject’s personal information.

In terms of POPIA, the Company, as a Responsible Party, is required to appoint an Information Officer (“**IO**”) and Deputy Information Officers (“**DIOs**”), to be responsible for establishing a POPIA Compliance Framework, and who following this, are required to assess, analyse and understand what types of personal information the Company is processing which belongs to Data Subjects and to thereafter develop certain processes and procedures, including a POPIA Policy, which have to be followed by all Company personnel when they process and use the personal information of third parties.

A Personal Information Impact Assessment as per the Company POPIA Compliance Framework has been carried out and created, which has indicated that the Company, during the course of its business activities does and will continue to collect, store and process personal information about the Company employees, its customers, suppliers and other third parties.

Furthermore, the Impact Assessment has defined and revealed that the Company processes different types of personal information including names, addresses, opinions, financial details, medical details and the like which pertain to current, past and prospective employees and customers, suppliers, and others who the Company communicates and deals with, and which processing is carried out for a variety of purposes, including for business, compliance and legal purposes.

The Company also processes special personal information including gender, sex, marital status, colour, age, race or ethnic origin, trade union membership and the like for the purposes of recruitment, employment equity reporting, legal compliance and for the facilitation of union fees and memberships.

Following the Personal Information Impact Assessment, the Company is satisfied that personal information is subject to the prescribed legal safeguards as specified in POPIA and other regulations.

This Policy, which applies to Libstar Holdings and its subsidiaries and divisions, sets out how all personnel at Libstar companies and subsidiaries (hereinafter referred to collectively as the “Company”) are to conduct the processing of and use of third-party information, which information needs to be processed lawfully and in accordance with POPIA.

## CONTENTS

---

1	STATEMENT FROM THE COMPANY BOARD OF DIRECTORS	4
2	INFORMATION PROCESSING TERMS AND DEFINITIONS	4
3	SCOPE AND APPLICATION	5
4	LAWFUL BASIS FOR PROCESSING	5
5	CONSENT	5
6	PURPOSE SPECIFIC	6
7	ACCURACY	8
8	DATA MINIMISATION	8
9	TRANSPARENCY AND PROCESSING NOTICES	9
10	GENERAL DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION	10
11	RECORDS MANAGEMENT DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION	11
12	RECORDS MANAGEMENT DUTIES: STORAGE OF RECORDS CONTAINING PERSONAL INFORMATION	12
13	RECORDS MANAGEMENT DUTIES: RETENTION AND DISPOSAL OF RECORDS HOUSING PERSONAL INFORMATION	14
14	OPERATORS	16
15	SHARING PERSONAL INFORMATION WITH THIRD PARTIES	17
16	CROSS BORDER TRANSFERS OF PERSONAL INFORMATION	18
17	DIRECT MARKETING	18
18	REPORTING PERSONAL INFORMATION BREACHES	19
19	DATA SUBJECT RIGHTS AND REQUESTS	20
20	THE RIGHT TO COMPLAIN	21
21	GOVERNANCE	22
22	TRAINING	22
23	NON-COMPLIANCE	23
24	VERSION AND AMENDMENTS	23

<b><u>ANNEXURE A</u></b>	<b>24</b>
<b>DOCUMENTS AND RECORDS CLASSIFICATION INSTRUCTIONS AND REGISTER FORMATS</b>	<b>24</b>
<b><u>ANNEXURE B</u></b>	<b>35</b>
<b>INCIDENT INVESTIGATION FORM</b>	<b>35</b>

## 1 STATEMENT FROM THE COMPANY BOARD OF DIRECTORS

- 1.1 The Company conducts business with the highest level of integrity, in accordance with the highest ethical standards and in compliance with applicable laws, including the Protection of Personal Information Act, 4 of 2013, (POPIA), which regulates the Processing of Personal Information.
- 1.2 The Protection of Personal Information Policy has been developed in order to provide clear guidance to all directors, employees and any persons who Process Personal Information on behalf of the Company in regard to how they are to Process Personal Information, thereby ensuring that all Personal Information is Processed by the Company in a lawful, transparent and consistent manner and in full compliance with all and any applicable data protection laws which may from time to time apply to its operations.
- 1.3 The Company requires compliance with all its policies, including this Protection of Personal Information Policy.

## 2 INFORMATION PROCESSING TERMS AND DEFINITIONS

POPIA makes use of certain terms and references that will be used in this Policy, which are explained below:

- 2.1 **“Company”** means Libstar Holdings Limited, a limited liability company incorporated in South Africa with registration number 2014/032444/06 and Libstar Operations (Pty) Ltd – registration number 2014/062496/07 and its subsidiaries;
- 2.2 **“Consent”** means in relation to POPIA, any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Information about them;
- 2.3 **“Data Subject”** means any individual or legal entity;
- 2.4 **“Operator”** means any person who Processes Personal Information on behalf of a Responsible Party as a contractor or sub-contractor, in terms of a contract or mandate, not subject to the direct authority of the Responsible Party;
- 2.5 **“Processing Notices”** means a notice setting out the prescribed information that must be provided to Data Subjects before collecting his, her or its Personal Information, (also known as “Section 18 POPIA notices”, “privacy notices” or “data protection notices”).
- 2.6 **“Personal Information”** means Personal Information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:
  - name, address, contact details, date of birth, place of birth, identity number, passport number;
  - bank details;
  - qualifications, expertise, employment details;
  - tax number;
  - vehicle registration;

- dietary preferences;
  - financial details including credit history;
  - next of kin / dependants;
  - education or employment history; and
- 2.7 **“Special Personal Information”**, includes race, gender, pregnancy, national, ethnic or social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, DNA analysis, retinal scanning and voice recognition.
- 2.8 **“Personnel”** means Company directors, employees and any other person who may Process Personal Information on behalf of the Company.
- 2.9 **“Processing, Process, Processed”** means in relation to Personal Information, the collection, receipt, recording, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; merging, linking, as well as restriction, degradation, erasure or destruction of information; or sharing with, transfer and further Processing, including physical, manual and automatic and in relation thereto which may be held on a **“Record”** which means any recorded information housing Personal Information Processed by the Company, or its Personnel, regardless of form or medium.
- 2.10 **“Purpose”** means the underlying reason why a Responsible Party or Operator needs to Process a Data Subject’s Personal Information.
- 2.11 **“Responsible Party”** means, in relation to POPIA, the person or legal entity who is Processing a Data Subject’s Personal Information.
- 2.12 **“Records”** means all documents and records housing data, including held, created, used or processed by the Company, including Records containing personal Information.

### 3 SCOPE AND APPLICATION

This Policy applies to any persons who Process Personal Information on behalf of the Company, including Company directors, employees and Operators, who will hereinafter be referred to collectively as “Personnel”.

### 4 LAWFUL BASIS FOR PROCESSING

In terms of POPIA, where Personal Information is Processed such Processing must be done lawfully and in a reasonable manner that does not infringe on the privacy of the Data Subject. In order to discharge the above obligations, Personnel must comply with the Processing guides, rules and procedures set out below.

### 5 CONSENT

- 5.1 A Data Subject does not have to Consent to the Processing of their Personal Information where there is a lawful basis for such Processing. A lawful basis for Processing in terms of the Data Processing laws, is where:

- the Processing is **necessary to conclude a contract** to which the Data Subject is a party and to perform contractual obligations or give effect to contractual rights;
  - the Processing is necessary in order to **comply with a law** or to comply with certain legal obligations imposed by a law;
  - the Processing is necessary to **protect Company's legitimate interests or rights, the Data Subject's legitimate interests or rights or a third party's legitimate interests or rights**, unless there is a good reason to protect the Data Subject's Personal Information that will override any such legitimate interests;
  - the Processing is necessary in order to perform a **public duty** or to perform tasks carried out in the public interest or the exercise of official authority.
- 5.2 Where there is no lawful basis for the Processing, then the Data Subject, has to Consent to the Processing.
- 5.3 Personnel must ensure that prior to Processing a Data Subject's Personal Information, that there is either a lawful reason for the Processing, or alternatively that the Data Subject has Consented to such Processing, which lawful reason will be described under the specific and informative Company Processing notices, or in the absence of a lawful reason, will call for the Data Subject's consent.
- 5.4 A Data Subject may withdraw their Consent as long as it provides the Company with a withdrawal of consent notice, which notice is available on the Company website. This notice will be handled and actioned directly by the duly appointed Company Information Officer or Deputy Information Officer and which outcome will be relayed to the respective Personnel who has been Processing such Personal Information.
- 5.5 A Data Subject may not withdraw Consent where no Consent is required, i.e., where the Company can show that there is a lawful basis for the Processing. In such a case the Data Subject may only object to such Processing, provided that an "Objection notice" is sent to the Company, which notice is available on the Company website. This request will be handled and actioned directly by the Information Officer or Deputy Information Officer and which outcome will be relayed to the respective Personnel who has been Processing such Personal Information.
- 5.6 Where a Data Subject withdraws Consent or objects to Processing, the Company and the respective Personnel who have been Processing the impacted Personal Information, will have to stop Processing the Personal Information, unless the Company can show compelling legitimate grounds for the Processing which overrides the interests, rights and freedoms of the Data Subject, or the Processing is necessary for the establishment, exercise or defence of legal claims.
- 5.7 The Information Officer or Deputy Information Officer will at the time of the withdrawal or objection referred to above, explain to the Data Subject the effects and consequences of any withdrawal or objection and relay the outcome to the respective Personnel who has been Processing such Personal Information.

## 6 PURPOSE SPECIFIC

- 6.1 Personal Information:

- may only be collected for a specified, explicit and legitimate purpose;
- must only be used for the purpose for which it was collected and for no other purpose, unless the Data Subject has been informed of the other purposes;
- may not be further Processed or used for any subsequent purpose unless that Personal Information is required for a similar purpose; and such Processing is compatible with the initial purpose.

6.2 The Company for the purposes of carrying out its business and related objectives, processes Personal Information belonging to a vast range of Data Subjects, including employees and staff, prospective employees and job applicants, students and interns, service providers and contractors, vendors, clients, customers, and other third parties, which processing is required for a variety of business-related purposes.

6.3 Examples of these purposes are described below:

- to recruit and employ - employment;
- to sell or purchase goods and services - procurement and supply chain;
- concluding and managing a contract or business transaction - contract;
- conducting criminal reference checks - legitimate interest;
- risk assessments - legitimate interest;
- insurance and underwriting purposes - legitimate interest;
- assessing and Processing queries, enquiries, complaints, and/or claims - legitimate interest;
- conducting credit checks - legitimate interest;
- confirming, verifying and updating personal details - legitimate interest;
- detection and prevention of fraud, crime, money laundering or other malpractices - legitimate interest;
- conducting market or customer satisfaction research - legitimate interest;
- direct marketing - marketing;
- audit and record keeping purposes - legitimate interest;
- managing debtor and creditors - legitimate interest;
- complying with laws and regulations - statutory;
- dealing with regulators - statutory;
- paying taxes - statutory;
- collecting debts or legal proceedings - statutory;
- communications - legitimate interest;
- managing employees - employment.

6.4 Company personnel must:

- ensure that before Personal Information is processed, there is a valid and legitimate reason for such processing; and
- advise all Data Subjects why the Personal Information is required, i.e., the purpose for the processing, which purpose will be described under the Company Processing notices, recorded on the Company website, which the Data Subject should be directed to.

## 7 ACCURACY

7.1 All Personal Information processed by the Company must be accurate and, where necessary, kept updated.

7.2 In order to ensure that Personal Information is accurate and is up to date, Personnel must:

- take all and every reasonable step to ensure that all Personal Information that they process is accurate, having regard to the purposes for which it is processed, and where it is found to be inaccurate, that it is where possible, updated and rectified without delay;
- implement procedures allowing Data Subjects to update their Personal Information;
- send out regular communications to Data Subject requesting “updates to details”, which if responded to, should be acted on immediately by the relevant or responsible department;
- where appropriate, and possible, ensure that any inaccurate or out-of-date records are updated, and the redundant information deleted or destroyed;
- take note of the rights of the Data Subject in relation to updates and rectifications of Personal Information, recorded under the Company Processing Notices and give effect to any update request, when such request has been communicated through to it by the Information Officer.

## 8 DATA MINIMISATION

8.1 The Company may not process Personal Information which is not necessary for the Purpose for which the Personal Information is processed.

8.2 Personnel must:

- ensure that when they process Personal Information on behalf of the Company, that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; and
- revisit all pre-populated questionnaires and forms which are currently used to collect or record Personal Information and consider the purpose or reason for the collection and thereafter analyse the types of Personal Information which is requested or collected and where of the view that certain Personal Information is not needed for the defined purpose, then such information should no longer be called for, collected and/or recorded and the relevant areas where this information is housed or asked for should be deleted.



## 9 TRANSPARENCY AND PROCESSING NOTICES

9.1 The Company has a duty to show that it has dealt with a Data Subject in a transparent manner.

9.2 In order to demonstrate transparency, the Company must refer all Data Subjects, to a specific and informed Processing Notice, at the time when the Company collects and processes a Data Subject's Personal Information or within a reasonable period thereafter, which Processing notice must set out:

- the types of Personal Information processed, and the purpose or reason for the processing;
- the lawful basis relied upon for such processing or whether consent is required for the processing;
- the period for which the Personal Information will be retained;
- who the Personal Information will be shared with, including external or cross border transfers and the mechanism(s) relied upon for such transfer;
- the security measures which are in place to protect the Personal Information, including where the Personal Information is sent to parties' cross border and the mechanism(s) relied upon for such protection; and
- the respective rights of the Data Subject and how these rights may be exercised.

9.3 In order to meet its obligations under 9.2 above, the Company has developed the following informed and specific Processing Notices, which apply to the different Data Subject categories with whom it has dealings with:

- a **Human Resources Processing Notice**, which applies to all employees – perspective and actual, all bursary or learnership beneficiaries - prospective or actual;
- a **Procurement and Supply Chain Processing Notice**, which applies to all participants in the Company supply chain, including persons who provide goods and services to the Company (service providers), persons or entities who purchase goods or services from Company (Customers), and/or other parties who the Company may engage with and who make up the Company procurement and supply chain, including Regulators;
- a **Company Secretarial Processing Notice**, which applies to all Data Subjects who deal with the Company from a company secretarial perspective, including directors, trustees, investors, Regulators, shareholders, stakeholders and/or other parties who the Company may engage with;
- a **Security Processing Notice**, which applies to any persons who come onto the Company sites, facilities and offices and who the Company may engage with;
- a **Website Privacy and Cookies Notice** which applies to any persons who make use of the Company websites, social media websites, emails, and other IT related communications facilities and platforms;

Processing Notices may be accessed on the Company website or can be requested from the Company's Information Officer. Processing Notice requests should be emailed to [popi@libstar.co.za](mailto:popi@libstar.co.za).

9.4 In order to give effect to the above transparency requirement, Personnel:

- must have an understanding of the provisions of the Data Processing laws;
- familiarise themselves with the abovementioned Company Processing Notices and any others that the Company may implement from time to time, and any changes made thereto;
- familiarise themselves with, where applicable, the Company standard binding corporate rules, its standard Personal Information transfer agreement and/or its Operator agreement;
- ensure that all Company documents, forms or other records (Records) that record or call for Personal Information contain the following Data Processing details:

Please note that in order for the Company to engage with you, it will have to Process certain Personal Information, which is your property, which Processing is described and explained under the specific and informative Company Processing Notices, recorded for ease of reference on the Company's website, which we ask that you download and read. By providing us with the required Personal Information, such act will be taken as an indication that you have read and agree with the provisions described under the Processing Notice and where applicable, you consent to the processing by us of your Personal Information.

- at the time of processing, direct the Data Subjects who you deal with to the applicable area of the Company website where the specific Company Processing notices are recorded.

## **10 GENERAL DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION**

10.1 In order to safeguard, secure and ensure the confidentiality and integrity of all Personal Information held by or under the control of the Company, the Company together with its Personnel must;

- identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;
- document the identified risks;
- establish, in response to the identified risks, reasonable technical and organisational measures across all areas where Personal Information is held or stored, including electronic and physical mediums;
- implement and maintain all approved and required measures across all areas where Personal Information is held or stored, including electronic and physical measures, all which are designed to minimise the risk of loss, damage, unauthorised destruction and/or unlawful access of Personal Information;
- regularly verify that these measures are effectively implemented; and ensure that the measures are continually updated in response to new risks or deficiencies in previously

implemented measures and safeguards, which measures include, where appropriate, among others, the following:

- the pseudonymisation and encryption of Personal Information;
- ongoing efforts to ensure the long-term confidentiality, integrity, availability and resilience of Personal Information recorded within the Company environment;
- applications and processes which have the ability to rapidly restore the availability of and access to Personal Information in the event of a tangible or technical incident; and
- procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures taken to ensure the security of Processing, including regular IT Security Audits.

10.2 The duty to ensure data privacy, confidentiality and integrity of Personal Information starts when the Company initially interacts with a Data Subject and will continue throughout the relationship, until the purpose for the Processing of the Personal Information comes to an end.

## **11 RECORDS MANAGEMENT DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION**

11.1 In order to ensure the confidentiality and integrity of all Records, especially those that record or contain Personal Information which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that:

11.1.1 all Processing of Personal Information activities and communications are reduced to writing and retained in a Record, which Record may either be electronic, or paper based;

11.1.2 each Record created is classified, and then is housed in a folder (Folder), and where applicable in sub folders of the Folder being a storage area, either electronic or paper based and in turn each Folder / subfolder is given an appropriate title or Folder name using the Company naming convention and classification guide and template set out under **“Annexure A”**;

11.1.3 Folders and Records must be named in a consistent and logical manner so they can be located, identified and retrieved as quickly and easily as possible;

11.1.4 all Folders and Records must be stored and saved in a way that the contents are safeguarded and are identifiable as per the agreed Company naming convention and classification;

11.1.5 the name of the Folder and related sub folders and Records held in such Folders, together with the classification thereof must be recorded in a department specific records register which has to be compiled for each department, using the Company standard department management register (hereinafter referred to as the **“Department Records Management Register”**), as set out under **“Annexure A”**, including the following details:

- classification;
  - the name of the Folder and related Records;
  - format of the Folder and related Records;
  - location of Record - including physical or electronic location;
  - who has access to the Folder, and the Records;
  - status of the Folder and the Records;
  - retention period pertaining to the Folder and/or Records; and
  - destruction date of the Records, when appropriate;
- 11.1.6 their respective department head reviews their own department specific Department Records Management Register annually to ensure compliance with this Policy;
- 11.1.7 each department provides a copy of its Department Records Management Register to the Information Officer, annually, or on request.
- 11.2 Upon termination of employment, or change of job roles or responsibilities of Personnel, the affected line manager responsible for such Personnel must ensure that all access rights to any Company Folders or Records is removed immediately and that all Company assets used to access the Folders and or Records are returned to the Company, and that all physical access rights to the Company premises and facilities are revoked or cancelled.

## **12 RECORDS MANAGEMENT DUTIES: STORAGE OF RECORDS CONTAINING PERSONAL INFORMATION**

- 12.1 In order to ensure the confidentiality and integrity of all paper-based Records that record or contain Personal Information, which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that all paper-based Records:
- which are housed in physical storage areas are labelled and the details recorded in the Department Management Register;
  - when in use, are not left around for others to access, and are not left in places where persons can view the contents e.g., on a printer or on unmanned desks;
  - are stored securely when not in use, in Folders, which in turn are placed in locked boxes, drawers, cabinets, or similar structures or containers;
  - that only Personnel who are required, on an operational and need to know basis, are given access to such Records and/or Folders; and
  - such Records and/or Folders are only removed from Company premises if such removal is recorded in the Department Records Management Register and when removed off site, such Records are safeguarded and kept confidential.
- 12.2 In order to ensure the confidentiality and integrity of all electronic Records that house or contain Personal Information, which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that:

- they comply with all applicable Company IT Policies and Procedures;
- all electronic Records are stored and housed on Company servers that are protected by approved security software, and one or more firewalls under the direction of the Company IT Manager, and where transferred or uploaded to cloud computing services from computers, devices and applications, that this is done in compliance with Company IT Policies and Procedures;
- all devices where electronic Folders and/ or Records are stored, are password protected and that passwords are not written down or shared, irrespective of seniority or department, which passwords must be strong passwords that are changed regularly. If a password is forgotten, it must be reset using the applicable method;
- all network devices and drives where electronic Folders and Records are stored have access control measures in place;
- electronic Folders and Records are not stored on mobile devices and removable media, which includes, but is not limited to smart phones, tablets and I pads, Digital media, USB sticks, external hard drives, CDs, DVDs, memory cards, tapes, unless the device is password protected and the content of such Record(s) is where possible encrypted;
- where one needs to use and access the contents of an electronic Folder or Record, off site, which will not be accessed using Company secured servers, and which will be downloaded on to portable device for off-site working purposes, such person must only remove the Folders and/or Records or parts thereof if such removal is recorded in the Department Records Register; only the record(s) which are necessary for one's immediate needs are removed; where possible and feasible, the Personal Information to be removed is strongly encrypted; and when removed off site, such Records are safeguarded and kept confidential and when no longer needed, that the removed Folder and/or Record, once dealt with is deleted from the portable device;
- all electronic Records are regularly backed up using the Company provided systems and applications and in accordance with backup protocols. Such backups will be tested regularly in line with the Company standard backup procedures and protocols under the direction of the IT Manager / Head of IT;
- all device screens, when not in use are always locked and password protected, especially when left unattended;
- electronic Records are only transmitted over secure networks, including wireless and wired networks.

12.3 In order to ensure the confidentiality and integrity of all Records that house or contain Personal Information, which are held by the Company, and in order to safeguard and secure these Records, Personnel must ensure that:

12.3.1 Records are shared with others on a “*need to know*” basis only. If Personnel are unclear on how to apply this requirement, the default position is that a conservative approach must be applied, i.e. information must be disclosed only to those people who have a legitimate business need for the information;

- 12.3.2 controls are in place to ensure that only personnel with proper authorisation and a need to know are granted access to Company systems and resources. Remote access shall be controlled through identification and authentication mechanisms;
- 12.3.3 proper controls are in place to authenticate the identity of Personnel or any third party who needs to access a Record, and all Personnel validate each person who requires access to the Record before allowing them access;
- 12.3.4 data used for authentication shall be protected from unauthorised access;
- 12.3.5 access to information classified as Special Personal Information or sensitive Personal Information must be provided only after the written authorisation of the Data Owner has been obtained, under an Onwards transmission notice. In this regard Personnel must refer all requests for access to the relevant Data Owners or their delegates for permission and signature of the Onwards transmission notice.
- 12.3.6 special needs for other access privileges will be dealt with on a request-by-request basis;
- 12.3.7 storage media containing Special Personal Information, or sensitive information (i.e. restricted or confidential information) shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the IT department.
- 12.4 Any attempts to bypass security controls or to obtain unauthorised access, or to make unauthorised use of another's account shall be considered a security breach or violation.
- 12.5 The use of any Company information or data for purposes other than for authorised business purposes shall be considered a security violation.
- 12.6 The use of any Company information or data for any unauthorised or illegal activity shall be considered a security breach or violation.
- 12.7 Any act, or failure to act, that constitutes or causes a security incident or creates a security exposure shall be considered a security breach or violation.
- 12.8 Any act, or failure to act that results in sensitive or business critical information being disclosed to an unauthorised person shall be considered a security breach or violation.
- 12.9 Any act, or failure to act that results in sensitive or business critical information being modified or destroyed, such that the Company is adversely impacted shall be considered a security breach or violation.
- 12.10 Any breach of this policy shall be considered a security breach or violation.

### **13 RECORDS MANAGEMENT DUTIES: RETENTION AND DISPOSAL OF RECORDS HOUSING PERSONAL INFORMATION**

- 13.1 Folders and Records housing Personal Information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless the longer retention of the Folder or Record:
- is required or authorised by law;

- is required by the Company for lawful purposes related to its functions or activities;
  - is required by a contract between the parties thereto; is as per consent received from the Data Subject who owns the Personal Information; or
  - is required for the Operational Requirements of the Company.
- 13.2 Records housing Personal Information may be retained indefinitely for business, historical, statistical or research purposes provided that the Company has established appropriate safeguards against the Records being used for any other purposes.
- 13.3 Each Company department will be responsible for the correct management of their Folders and Records, including the closing and archiving of these Records when they are no longer required.
- 13.4 In order to ensure that the above duties are discharged, all Personnel must ensure that:
- on an ongoing basis they manage the respective life cycles of Folders and Records under their control;
  - they establish what record retention periods and related requirements apply to the respective Folders and Records under their control, as per the Company Records Retention Policy;
  - the record retention periods, and related requirements are recorded in the department's relevant Department Records Management Register;
  - a Folder and Record is formally closed when the matter housed in the Folder or Record comes to an end, which is documented in the relevant Document Management Register;
  - a closed Folder or Record is moved to a dedicated archive storage area where the Folder or Record will be retained for the required retention period;
  - Folders and Records are only archived in secure storage media;
  - only authorised personnel are granted physical and system-based access to archived Folders and Records;
  - Folders and Records are archived in areas that are regularly backed up;
  - once the prescribed retention period in respect of an archived Folder or Record has expired, the Folder or Record is marked "for deletion or disposal";
  - before a Folder or Record is deleted or destroyed, the department head must obtain permission to delete or destroy said Folder or Record from the Information Officer, which will be reflected in the relevant department Records Management Register;
  - each department, once approval for the deletion / destruction of the Folder or Record has been received, will be responsible for the deletion or destruction of such archived Folder or Record after the expiration of the retention period, unless instructed

otherwise by the Information Officer, for example when there is a requirement to place the Folder or Record under a legal or PAIA hold;

- the legal / PAIA hold status must be indicated under the relevant Folder or Record in the relevant Document Management Register;
- during a legal / PAIA hold procedure, the affected Folder or Record must not be destroyed, even if the retention period has expired;
- the deletion / disposal of Folders and Records must ensure the permanent and complete deletion / disposal of all originals and reproductions (including both paper and electronically stored records);
- the department head is responsible for documenting the destruction details under the relevant department Records Management Register.

## **14 OPERATORS**

14.1 Where the Company makes use of an Operator, in terms of Sections 19-21 of POPIA, it must ensure that the Operator only uses the Personal Information per the mandate to Process issued by the Company, keeps the Personal Information placed under its control, confidential, secure and safe, and that a standard Company Operator Agreement / Addendum (hereinafter referred to as the "Operator Agreement / Addendum") is concluded between the Company and the Operator. This Agreement sets out the above provisions and any other terms and rules which the Operator will have to follow when Processing Personal Information on behalf of the Company, and which Operator Agreement / Addendum is recorded on the Company website.

14.2 All Personnel must:

- familiarise themselves with the standard Company Operator Agreement / Addendum;
- ascertain who they use as Operators, now and in the future, include such details under an Operator register, and ensure that all such Operators sign the standard Company Operator Agreement / Addendum or a similar one which has been approved;
- ensure that Operator Agreement / Addendum is followed by an Operator and that where an Operator Agreement / Addendum is breached, bring this to the attention of one's line manager and the Information Officer and following a decision reached by these parties, carry out the planned course of action, which ultimately must aim to protect and secure the Personal Information which is the subject matter of that Operator Agreement / Addendum.

## **15 SHARING PERSONAL INFORMATION WITH THIRD PARTIES**

15.1 The Company may not share Personal Information with third parties, unless:

- there is a legitimate business need to share the Personal Information; or
- the Data Subject has been made aware that their Personal Information will be shared with others and has, where required, given consent to such sharing; or



- the person receiving the Personal Information has agreed to keep the Personal Information confidential and to use it only for the purpose for which it was shared under the standard Company Personal Information transfer agreement or where acting as an Operator.

15.2 In order to ensure that the above takes place, Personnel must ensure:

- that where Personal Information is shared externally with a third party, there is a legitimate business need to share the Personal Information; or the Data Subject has been made aware that their Personal Information will be shared with others and has, where required, given consent to such sharing;
- in the absence of the above two situations, has signed the standard Company Personal Information transfer agreement, which is concluded with the recipient, before receipt of the Personal Information;
- that where Personal Information is shared with an Operator, that the standard Company Operator Agreement / Addendum is concluded with the Operator before receipt of the Personal Information;
- that any requested deviations for the standard Company Personal Information transfer agreement or the Operator Agreement / Addendum is vetted and approved by the Group HR or Group Internal Auditing departments beforehand;
- when sending emails that contain Personal Information, that they are marked “confidential”, do not contain the Personal Information in the body of the email, whether sent or received, but rather placed in an attachment, which attachment is password protected or encrypted before being transferred electronically;
- that Personal Information is not transferred or sent to any entity not authorised directly to receive it;
- that where Personal Information is to be sent by facsimile transmission, that the recipient has been informed in advance of the transmission and that he or she is waiting by the fax machine to receive the data;
- that where Personal Information is transferred physically, whether in hardcopy form or on removable electronic media, that it is passed directly to the recipient or sent using recorded deliver services and housed in a suitable container marked “confidential”;
- that where Personal Information is shared internally, that adequate measures are put in place to protect the confidentiality and integrity of such information.

## **16 CROSS BORDER TRANSFERS OF PERSONAL INFORMATION**

16.1 The Company may not transfer Personal Information to another party who is situated outside South Africa, unless:

- the Data Subject Consents (under POPIA);

- the transfer is necessary in order to perform a contract between Company and a Data Subject, or for reasons of public interest, or to establish, exercise or defend legal claims or to protect the vital or legitimate interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent;
- the country where the Personal Information is being transferred to, provides the Data Subject with the same level of protection as is housed under the data processing laws applicable in South Africa; or alternatively
- the Company has concluded a Personal Information data transfer agreement with the recipient of the Personal Information, either in the form of a standard binding corporate rule, or an Operator Agreement / Addendum or a Personal Information transfer agreement, which sets out the rules that apply to the receipt and the subsequent Processing of that Personal Information.

16.2 In order to ensure that the above is followed, Personnel may not transfer Personal Information to areas outside South Africa, unless one of the following controls and safeguards are in place:

- the South African Data Privacy /Personal Information Regulator has issued an “adequacy decision” confirming that the territory or country where the Company proposes transferring the Personal Information to, has adequate Data Protection laws in place which will afford the Data Subject with the same level of protection as that under POPIA;
- the standard Company Personal Information data transfer agreement or Operator Agreement / Addendum has been concluded with the recipient of the Personal Information;
- the Data Subject has given Consent (POPIA) to the proposed transfer, having been fully informed of any potential risks; or
- the transfer is necessary in order to perform a contract between the Company and a Data Subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent (POPIA).

## **17 DIRECT MARKETING**

17.1 Direct marketing, including unsolicited direct electronic marketing is prohibited unless the Data Subject has consented to the receipt of this marketing material.

17.2 In order to ensure that direct marketing is sent out in a lawful manner, all Personnel must ensure that:

- all Company customers, when approached or dealt with for the first time, are given the opportunity in an informal manner to agree or disagree to the receipt of any Company direct marketing material and that where consent is granted, that the details of the customer are set out under a “consented to” direct marketing data base, and when marketing material is sent to these Data Subjects, that the material houses an “opt out” form, allowing the Data Subject to opt out of any further marketing material should it so elect;

- before direct marketing is sent to a non-customer that such person provides their consent thereto, which will be in the form of the prescribed “opt in” notice, available on the Company website;
- when marketing material is sent to Data Subjects, who have “opted in” that the material contains an “opt out” form, allowing the Data Subject to opt out of any further marketing material; and
- when a Data Subject exercises their right to object to receiving direct marketing, in the form of an opt out, that such opt out is recorded and given effect to, and that no further direct marketing is sent to the opted-out customer.

17.3 All Personnel, especially those who engage in direct marketing must familiarise themselves with the Company marketing opt in and opt out requirements.

## 18 REPORTING PERSONAL INFORMATION BREACHES

18.1 In the event of a Personal Information breach, the Company has a duty to give notice of such breach to the Regulator who is in charge of POPIA, being the *Information Regulator*, and to the Data Subject(s) whose Personal Information has been affected as a result of such breach.

18.2 The Company has put in place appropriate procedures to deal with any Personal Information breach and will notify the Information Regulator and/or the Data Subjects, as the case may be, when it is legally required to do so of any breach.

18.3 Personnel have a duty to:

18.3.1 immediately report through to the Information Officer, any suspected or known Personal Information breach; using the prescribed Company data breach report, which report format is annexed hereto marked “**Annexure B**” . The report must contain the following details:

- categories and approximate number of Data Subjects concerned;
- categories and approximate number of Personal Information records concerned;
- the likely cause of and the consequences of the breach; and
- details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

18.3.2 keep such information strictly private and confidential;

18.3.3 ensure that they do not deal with any persons in relation to the Personal Information breach, including any officials or investigators, noting that only the Information Officer with the approval of the CEO or the Company’s Board has the right to report any Personal Information or security breach to the Information Regulator and/or the affected Data Subjects, as the case may be and to deal with any person in connection with such matter.

## 19 DATA SUBJECT RIGHTS AND REQUESTS

19.1 A Data Subject has rights under POPIA in relation to their Personal Information, including the right to:

- withdraw Consent;
- object to Processing;
- obtain confirmation of Processing and/or access to Personal Information;
- amend, update and delete Personal Information;
- object to direct marketing;
- be notified of a personal information breach; and
- complain about the processing of Personal Information.

19.2 The Company has developed and will maintain certain processes and related forms that give effect to these Data Subject rights. When a Data Subject is desirous of exercising these rights, then they must be directed to the Company website at <https://www.libstar.co.za/legal/>, where the relevant Processing Notices and related prescribed forms are housed. Forms, once completed, must be directed to and handled directly by the Information Officer or his or her deputy, who will be responsible for dealing with the request and advising the affected Data Subject and/ or any affected Personnel of any decision and outcome in relation to such request.

19.3 Personnel must:

- familiarise themselves with the Data Subjects' rights, and the related processes and forms which need to be followed and completed in order to access these rights;
- take note of and give effect to these processes;
- in particular note that where a Data Subject seeks advice on what Personal Information the Company holds and which pertains to that Data Subject or where the Data Subject is desirous of accessing this Personal Information, that such right has to be exercised using the "request for access to information" procedure which is described in the Promotion of Access to Information Act, 2 of 2000, ("PAIA"), and which request procedure is more fully set out under the Company's PAIA Manual available on the Company website.
- where asked by any Data Subject to give effect to these rights, not deal with the request directly but instead direct the Data Subject to the relevant process and form on the Company website and aid in so far as completing the form only.

## 20 THE RIGHT TO COMPLAIN

20.1 A Data Subject has the right to lodge a complaint with regards to the Processing of their Personal Information.

20.2 The Company has established for this purpose, an internal compliant resolution procedure.

- 20.3 Should a Data Subject wish to submit a complaint, Personnel must, if contacted by the Data Subject, ask the Data Subject to complete the prescribed “personal information processing complaint” form, which is housed on the Company website, and to submit the completed complaint form directly to the Information Officer.
- 20.4 On receipt of the complaint, the Information Officer will attempt to hear and resolve the matter internally and failing resolution will provide the Data Subject with a non-resolution notice.
- 20.5 If the Information Officer and Data Subject are able to resolve the matter, a record setting out the solution will be compiled, and signed by the parties and any other affected persons provided with details of the resolution.
- 20.6 Where the parties are unable to resolve the matter, the Data Subject on receipt of the non-resolution notice, will have the right to refer the complaint to the Information Regulator.

## **21 GOVERNANCE**

- 21.1 The Company has appointed Information Officer(s) and Deputy Information Officer(s), as outlined in the list provided on our website, who will be responsible for the following:
- developing, constructing and once prepared, implementing and overseeing an enterprise-wide Personal Information Processing framework and related roadmap including various Personal Information Processing procedures and policies, including this Policy;
  - monitoring compliance with this Policy, the various Personal Information Processing procedures and the Data Processing law;
  - providing all Personnel with the necessary and required Personal Information Processing training;
  - providing ongoing guidance and advice on Personal Information Processing;
  - conducting Personal Information impact assessments when required, including base line risk assessments of all the Company’s Personal Information Processing activities;
  - ensuring that all operational and technological Personal Information and data protection standards are in place and are complied with;
  - working closely with IT in order to ensure that appropriate technological and operational measures have been implemented in order to ensure the safety and security of all electronically stored Personal Information;
  - receiving and considering reports from IT about compliance with all technological and operational data protection standards and protocols;
  - be entitled and have authorisation in conjunction with the Company HR function, to initiate disciplinary proceedings against Personnel who breach any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise), including this Policy;

- review and approve any contracts or agreements which deviate from the standard Company Processing documentation;
- attend to requests and queries from Data Subjects, including requests for access to their Personal Information;
- liaising with and/or co-operating with any regulators or investigators or officials who may be investigating a Personal Information or data privacy matter.

21.2 All queries and concerns in relation to the Processing of Personal Information within the Company operations or concerning Company activities, must be taken up with the Information or Deputy Information Officers.

21.3 The Company's IT department will be responsible for the following:

- conducting cyber security risk assessments including base line risk assessments of all the Company information technology activities;
- ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place in order to address all IT security risks;
- ensuring that all systems, services and equipment used for Processing and/or storing data adheres to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards;
- issuing appropriate, clear, and regular rules and directives, whether for the Company as a whole or a particular part of it, department, person or level of person in relation to any aspect of the Company work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like.
- evaluate any third-party services which the Company is considering or may acquire to Process or store data, e.g., cloud computing services and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place in order to address all IT security risks which may present themselves in respect of these external service providers.

## 22 TRAINING

22.1 The Company will conduct regular training sessions covering the contents of the data privacy laws and the Company related Personal Information Processing policies and procedures, which will be available to all Personnel.

22.2 Personnel must:

- attend the scheduled and offered training;
- do all that is necessary in order to understand the data privacy laws and how they may impact on the Company Personal Information Processing activities;

- familiarise themselves with the Company Personal Information Processing policies, procedures and prescribed forms;
- ensure that they Process Personal Information in accordance with the Data Processing laws, this Policy, the training, the related policies and procedures and/or any guidelines issued by the Company from time to time.

## **23 NON-COMPLIANCE**

- 23.1 Compliance with this Policy and any related procedures and policies is mandatory.
- 23.2 Any transgression of this Policy, and any related procedures and policies, will be investigated and may lead to action being taken against the transgressor.

Further information on the relevant data protection laws, POPIA, the Company Processing of Personal Information procedures and issues, and Processing Notices, including specific practical guidance on issues of particular relevance to Personnel, can be found on the Company's website.

## **24 VERSION AND AMENDMENTS**

This Policy is effective as of 22 July 2021.

The Company reserves the right to amend the Policy at any time, for any reason, and without notice to you other than the posting of the updated Policy on the Company Website.

We therefore request that you to visit our website frequently in order to keep abreast with any changes.

Reviewed on 19 June 2024

## **DOCUMENTS AND RECORDS CLASSIFICATION INSTRUCTIONS AND REGISTER FORMATS**

### **CLASSIFICATION INSTRUCTIONS**

Any person who collects, uses, stores, or transmits Documents and Records has a responsibility to maintain and safeguard such Data.

The first step in establishing the safeguards that are required for a particular type of Documents and Records is to determine the level of sensitivity applicable to such Data. Documents and Records classification is a method of assigning such categories and thereby determining the extent to which the Documents and Records needs to be governed, controlled and secured.

The responsibility for the classification of Documents and Records rests with the Documents and Records owner / business unit where the documents have their origin.

Documents and Records classification, in the context of information security, also addresses the impact to the Group should such classified Documents and Records be disclosed, altered, or destroyed without authorisation.

The classification of Documents and Records helps determine what baseline security controls are appropriate for safeguarding that Data. All Group Documents and Records are categorised into one of four sensitivity classifications:

#### **Proprietary Data**

Documents and Records should be classified as Proprietary when this information is restricted to management approved internal access and protected from external access. Unauthorised access could influence the Company's operational effectiveness, cause a financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is therefore vital.

Examples of this type of Documents and Records includes passwords and information on corporate security procedures; know-how used to process client information; Standard Operating Procedures used in all areas of Company business; all Company-developed intellectual property, whether used internally or in transactions with third parties.

#### **Confidential Documents and Records**

Documents and Records should be classified as Confidential when the unauthorised disclosure, alteration or destruction of that Documents and Records could cause a significant level of risk to the Company or its affiliates. Examples of Confidential Documents and Records include Documents and Records protected by privacy regulations and Documents and Records protected by confidentiality agreements. This also includes information received from third parties in any form for processing and use by any Group Company. The highest level of security controls should be applied.

Access to Confidential Documents and Records must be controlled from creation to destruction and will be granted only to those persons affiliated to the respective Group Company who require such access to perform their job ("need to know"). Access to Confidential Documents and Records must be individually requested and then authorised by the Documents and Records Owner who is responsible for the data.



Confidential Documents and Records is highly sensitive and may have personal privacy considerations or may be restricted by a statute. In addition, the negative impact on the institution should this Documents and Records be incorrect, improperly disclosed, or not available when needed is typically very high.

Examples of Confidential / Restricted Documents and Records include salaries and other personnel data; accounting Documents and Records and internal financial reports; Company business plans; confidential customer business Documents and Records; confidential contracts; and any information shared in respect thereof.

Such Confidential Documents and Records shall also be protected in terms of the Protection of Personal Information Act, 4 of 2013, and in accordance with the Company POPIA Policy.

### **Internal / Private Documents and Records**

This type of Documents and Records can be defined as any information that is proprietary or produced only for use by members of the Group who have a legitimate purpose to access such data.

Documents and Records should be classified as Internal / Private when the unauthorised disclosure, alteration or destruction of that Documents and Records could result in a moderate level of risk to the Company or its affiliates. By default, all information assets that are not explicitly classified as Confidential or Public Documents and Records should be treated as Internal / Private Data. A reasonable level of security controls should be applied to Internal Data.

Access to Internal / Private Documents and Records must be requested from, and authorised by, the Documents and Records Owner who is responsible for the data. Access to Internal / Private Documents and Records may be authorised to groups of persons by their job classification or responsibilities (“role-based” access) and may also be limited by one’s department.

Internal / Private Documents and Records is moderately sensitive in nature. Often, Internal / Private Documents and Records is used for making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on the Group should this information not be available when needed is typically moderate. Examples of Internal / Private Documents and Records include official Company records such as financial reports, human resources information, some research data, unofficial employee records, budget information, internal operating procedures and operational manuals, internal memoranda, emails, reports and other documents, and technical documents such as system configurations and floor plans.

### **Public Documents and Records**

This type of Documents and Records can be defined as any information that may or must be made available to the public, with no legal restrictions on its access or use.

Documents and Records should be classified as Public when the unauthorised disclosure, alteration or destruction of that Documents and Records would result in little or no risk to the Company and its affiliates. While little or no controls are required to protect the confidentiality of Public Data, some level of control is required to prevent unauthorised modification or destruction of Public Data.

Public Documents and Records is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of Public Documents and Records should be

protected. The appropriate Documents and Records Owner must authorise replication or copying of the Documents and Records to ensure it remains accurate over time. The impact on the company, should Public Documents and Records not be available is typically low (inconvenient but not debilitating). Examples of Public Documents and Records include directory information, course information and research publications.

## **DATA COLLECTIONS**

Data Owners may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of an employee's address and ID number, the data collection should be classified as Confidential even though the employees name and address may be considered Public Data.

## **DETERMINING CLASSIFICATION**

The aim of information security is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the Group if confidentiality, integrity or availability of the data is compromised.

POTENTIAL IMPACT	LOW	MODERATE	HIGH
<b>Security Objective</b>			
<b>Confidentiality</b> - Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorised disclosure of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.
<b>Integrity</b> - Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.
<b>Availability</b> - Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organisational operations, organisational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.

## INFORMATION HANDLING REQUIREMENTS

The table below defines the required security controls for handling, transmitting, dispatching, protecting, and reproducing classified information assets:

SECURITY CONTROL	INFORMATION CLASSIFICATION			
	Area	Proprietary Data	Confidential	Internal / Private Data
Access Control	<p>Viewing and modification restricted to authorised individuals as needed for business-related roles.</p> <p>Data Owners or custodian grants permission for access, plus approval from line manager.</p> <p>Authentication and authorisation required for access.</p> <p>Confidentiality agreement required.</p>	<p>Viewing and modification restricted to authorised individuals as needed for business-related roles.</p> <p>Data Owners or custodian grants permission for access, plus approval from line manager.</p> <p>Authentication and authorisation required for access.</p> <p>Confidentiality agreement required.</p>	<p>Viewing and modification restricted to authorised individuals as needed for business-related roles.</p> <p>Data Owner or custodian grants permission for access, plus approval from the line manager.</p> <p>Authentication and authorisation required for access.</p>	<p>No restrictions for viewing.</p>
Copying and Printing (applies to both paper and electronic)	<p>Data shall only be printed when there is a legitimate need.</p> <p>Copies shall be limited to individuals authorised to access the data and have signed a confidentiality agreement.</p> <p>Information shall not be left unattended on a printer / desk.</p> <p>Control access to print output on copier.</p>	<p>Data shall only be printed when there is a legitimate need.</p> <p>Copies shall be limited to individuals authorised to access the data and have signed a confidentiality agreement.</p> <p>Information shall not be left unattended on a printer / desk.</p> <p>Control access to print output on copier.</p>	<p>Data shall only be printed when there is a legitimate need.</p> <p>Copies shall be limited to individuals on a need-to-know basis.</p> <p>Information shall not be left unattended on a printer / desk. Control access to print output on copier.</p>	<p>No restrictions</p>

	Copies shall be labelled as per categorisation "Confidential" or "Proprietary".	Copies shall be labelled as per categorisation "Confidential" or "Proprietary".		
Physical Security	<p><b>Hardcopy:</b> Secure in locked cabinet or location with appropriate physical controls.</p> <p>Physical access shall be monitored, logged, and to authorised individuals.</p>	<p><b>Hardcopy:</b> Secure in locked cabinet or location with appropriate physical controls.</p> <p>Physical access shall be monitored, logged, and to authorised individuals.</p>	<p><b>Hardcopy:</b> Secure in locked cabinet or location with appropriate physical controls.</p>	System shall be locked or logged out when unattended.
Information storage	<p>Storage on a secure server, cloud <b>recommended.</b></p> <p>Storage in a secure data Centre or cloud <b>recommended.</b></p> <p>Should not store on an individual's workstation, mobile device (cell phones, laptops, iPad, etc.) or removal devices (USB, external hard drives). If stored on a workstation or mobile device, shall use full disk encryption.</p> <p>Encryption on backup media required.</p> <p>Use restricted access folders.</p> <p><b>Mandatory:</b> file password protection for sensitive files at document level.</p>	<p>Storage on a secure server or cloud <b>recommended.</b></p> <p>Storage in a secure data Centre or cloud <b>recommended.</b></p> <p>Should not store on an individual's workstation, mobile device (cell phones, laptops, iPad, etc.) or removal devices (USB, external hard drives).</p> <p>Hardcopy: Secure in locked cabinet or location with appropriate physical controls.</p> <p>Use restricted access folders.</p> <p><b>Mandatory:</b></p>	<p>Storage on a secure server or cloud <b>recommended.</b></p> <p>Storage in a secure data Centre or cloud <b>recommended.</b></p> <p>Lock screen when unattended.</p>	<p>Storage in a secure server recommended.</p> <p>Storage in a secure Data Centre.</p> <p>Lock screen when unattended.</p>

	Hardcopy: Secure in locked cabinet or location with appropriate physical controls.	file password protection for sensitive files at document level.		
Transmission	Encryption required.  Cannot transmit via email unless encrypted and secure with a digital signature.	Encryption required	Encryption required	No restrictions
Remote access to systems hosting data	Access restricted to local network or VPN.  Confidentiality agreement required for remote access by third party for technical reasons.	Access restricted to local network or VPN.	Access restricted to local network or VPN.	No restrictions

**DOCUMENT RECORDS MANAGEMENT REGISTER FORMAT**

<b>Author:</b> Your name	
<b>Title:</b> Name of your project	
<b>Duration:</b> Dates of project	
<b>Classification:</b> <i>See definitions above</i>	
<p><b>1. File Structure</b></p> <ul style="list-style-type: none"> <li>Describe the organisation of computer folders for your project.</li> <li>List the primary folders, and then summarise the organisation of their sub-folders.</li> <li>How will the computer folders for your project be distinguished from other projects and work that you might be involved with?</li> </ul> <p><b>Good Practice</b></p> <ul style="list-style-type: none"> <li>Use a system that is logical to you, but simple and self-explanatory to others.</li> <li>Avoid using the same name for sub-folders as this may lead to the over writing of their contents.</li> </ul>	
<b>2. File Names housed in folder</b>	
<b>Primary Folder name</b>	<b>Location</b>
<b>Sub Folder name</b>	<b>Contents</b>
<b>Sub Folder name</b>	<b>Contents</b>
<b>Sub Folder name</b>	<b>Contents</b>
	<b>Signed:</b> <b>Version:</b>
<b>Date Created:</b>	<b>Date amended:</b>

**DOCUMENT RECORDS MANAGEMENT REGISTER FORMAT**

**COMPANY:**

**DEPARTMENT NAME:**

**DEPARTMENT DETAILS:**

**AREA WHERE SITUATED:**

**HEAD OR MANAGER OF DEPARTMENT:**



REF. NO	CATEGORY	NAME OF FILE	SPECIAL PERSONAL INFORMATION	PERSONAL INFORMATION	STATUS AND DATES	FORMAT & LOCATION SERVER / SYSTEM	DETAILS OF PERSONS WHO HAVE ACCESS	ARCHIVE PERIOD	SPECIFIC INSTRUCTION / INFORMATION	DESTROYED
<b>CLASSIFICATION</b>										
Dept- HR	Employees  <b>Folder:</b> Current Employees	<i>Alison Lee</i>	Yes	Yes	<b>Current / Archived</b>  <b>Date:</b> 1/02/2019	<b>Hard file</b> <i>Detail location</i>	Person A Person B Person C	7 years	i.e. Legal or PAIA Hold  Off Site Storage	Date:  Manner:  Company (where applicable):  Permission by:  Authorisation signature:
						<b>Electronic</b> <i>Detail location</i>		Indefinite		
						<b>Copies</b> <i>Detail location</i>		Location		

**Note:**

The records maintained by this department were reviewed on .....

New records should be added to this schedule and those no longer being filed must be deleted in accordance with this Policy and the Records Retention and Archive Policy.

**Company:**

**Department:**

**Valid for:**

**Responsible person:**

**Signed off by Information Officer:**

**INCIDENT INVESTIGATION FORM**

This incident report is to be used for all incidents relating to privacy and information security incident management.

Definition of an incident: A threat or event that compromises, damages, or causes a loss of confidential or protected information.

Confidential information: includes proprietary, technical, business, financial, joint-venture, customer and employee information that is not available publicly. It is the employee's responsibility to know what information is confidential and to obtain clarification when in doubt.

Person reporting the incident (can remain anonymous)	
Manager	
Date and time incident occurred	
Date and time incident reported	
Division	
Site	

**INCIDENT SUMMARY (SHORT STATEMENT OF EVENT)**


**INCIDENT INVESTIGATION**

The following sections are intended to assist you to clarify the sequence of events immediately preceding the incident. They expand on the details already provided in the summary. Additional pages/ documents can be attached where required.

**WHO WAS INVOLVED?**


**ARE THERE WITNESSES?**


**WHAT HAPPENED?**


**WHEN DID THE INCIDENT OCCUR?**


**WHERE DID THE INCIDENT OCCUR?**



**THE EXISTENCE OR LOCATION OF ANY PROOF THAT MAY EXIST?**


**THE EXTENT OR CONSEQUENCES OF THE DAMAGE / COMPROMISE**


Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## **POPIA DOCUMENTS IN SUPPORT OF THE ABOVE POLICY**

1. POPIA Compliance Framework
2. Appointment of Information Officer(s) (IO) and Deputy Information Officer(s) (DIO)
3. Personal Information Impact Assessments and Data Maps (where applicable)
4. Processing Notices
5. Operator Agreement
6. Sub-Operator Agreement
7. Data Transfer Agreement / Cross border Agreement
8. Binding Corporate Rules (where applicable)
9. Forms:
  - Form 1-Objection to the Processing of Personal Information
  - Form 2-Request for Correction or Deletion
  - Form 4-Opt-in-Request for Consent to Process Personal Information
  - Form 5-Complaint
  - Form 5A-Internal Complaint
10. PAIA Manual