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 the 1st July 2021, is a law that regulates the use and Processing of a person's and/or legal entity's Personal Information, this being in response to, and to protect and give effect to a person's and/or legal entity's rights to privacy, including the right not to have their / its Personal Information and related data misused, abused or used for ulterior Purposes.

POPIA applies to Personal Information which belongs to person's and/or legal entities ("Data Subjects") which is Processed, be it in an automated or non-automated manner in South Africa, by another ("Responsible Party") and places on any Responsible Party who is Processing a Data Subject's Personal Information, a duty to use it lawfully and only for a specific and defined Purpose(s).

In terms of POPIA, the Gauteng Infrastructure Financing Agency ("the Agency") as a Responsible Party, is required to appoint an Information Officer ("IO") and Deputy Information Officer ("DIO"), herein collectively referred to as "the Information Officer" to be responsible for establishing a POPIA Compliance Framework, and who following this, is required to assess, analyse and understand what types of Personal Information the Agency is Processing which belongs to Data Subjects and to thereafter develop certain Processes , including a POPIA Policy ("Policy"), which have to be followed by all units and Personnel" when they Process and use another's Personal Information.

A Personal Information Impact Assessment as per the Agency's POPIA Compliance Framework has been carried out and created, which has indicated that the Agency, during its business activities, does and will continue to collect, store and Process Personal Information about the Agency, employees, its customers, service providers, and other third parties.

Furthermore, the Impact Assessment has defined and revealed that the Agency Processes a large number of different types of Personal Information, including names, addresses, opinions, financial details, medical details, and the like, which pertain to current, past, and prospective employees, customers, service providers, and others who the Agency communicates and deals with and which Processing is carried out for a variety of Purposes, including for business, compliance and legal Purposes.

The Agency also Processes Special Personnel Information including gender, sex, marital status, colour, age, race or ethnic origin, religious beliefs, trade union membership, and the like for recruitment, employment equity statistics, legal compliance, the facilitation of union fees, memberships and employment verifications.

Following the Personal Information Impact Assessment, the Agency is confident that while this Personal Information is held on paper or a computer or other media, such storage is subject to the prescribed legal safeguards as specified in POPIA and other regulations.

This Policy, sets out how the Agency and its Personnel are to go about Processing and using another's Personal Information, which information needs to be Processed lawfully and by following the provisions of POPIA.

CONTENTS

ABBREVIATIONS

CD	Compact Disk
DIO	Deputy Information Officer
DNA	Deoxyribonucleic Acid
DVD	Digital Video Disk
EU	European Union
GIFA	Gauteng Infrastructure Financing Agency
IO	Information Officer
IT	Information Technology
USB	Universal Serial Bus

1. STATEMENT FROM THE AGENCY

1.1 The Agency has a long and proud tradition of conducting business with the highest level of integrity, by following the highest ethical standards and in full compliance with all applicable laws, including the law known as the POPIA, which regulates the Processing of Personal Information.

1.2 This Policy is developed at the direction of the compliance unit in the Agency to provide clear guidance to the Agency, and those units and Personnel who Process Personal Information on behalf of the Agency ("Operators") on how they are to Process Personal Information, thereby ensuring that all Personal Information Processed is done 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, including POPIA and the General Data Protection Regulation 2016/679 (GDPR) applicable in the European Union (EU) (hereinafter referred collectively as the "data protection laws").

1.3 The Agency 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, which is used in this Policy, which is explained below:

2.1 **"Agency"** means the Gauteng Infrastructure Financing Agency, units and Personnel;

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 clear positive action, signify agreement to the Processing of Personal Information about them;

2.3 **"Compliance Framework"** means an established framework mapped to the Agency's POPIA Policy, which predefines Processes on how to Process Personal Information, enabling Data Subjects' the right to the protection of Personal Information;

2.4 **"Data Subject"** means any individual / person or legal entity;

2.5 **"Impact Assessment"** means the assessment carried out, which indicates how the Agency collects, stores, and Processes Personal Information and its impact on the Agency's employees, its customers, service providers, and other third parties;

2.6 **"Information Officer"** means collectively the Information Officer including the duly delegated Deputy Information Officer, who must be appointed in writing by the Agency and registered with the Information Regulator;

2.7 **"Information Regulator"** means the body which is empowered to monitor and enforce compliance by public and private bodies with the provision of the POPIA;

2.8 **Onwards Transmission Notice"** means the onward transmission or sharing of Personal Information that is necessary for the pursuance or protection of the Agency's legitimate interests or that of the Data Subject or any third party;

2.9 **"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, without coming under the direct authority of the Responsible Party;

2.10 **"Operator Agreement"** means the agreement that governs the relationship between a Responsible Party and the Operator.

2.11 **"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").

2.12 **"Policy"** means this policy on the Processing of Personal Information framework developed for the Agency;

2.13 **"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
- **Special Personal Information**, being 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, Deoxyribonucleic Acid ("DNA") analysis, retinal scanning and voice recognition.

2.14 **"Personnel"** means the Agency's, employees, and any other person who may Process Personal Information on behalf of the Agency.

2.15 "**Processing, Process, Processed, Processes**" 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 there to which may be held on a **"Record"** which means any recorded information housing Personal Information Processed by the Agency regardless of form or medium.

2.16 **"Purpose"** means the underlying reason why a Responsible Party or Operator needs to Process a Data Subject's Personal Information.

2.17 **"Responsible Party"** means, in relation to POPIA, the person and/or legal entity who is Processing a Data Subject's Personal Information.

2.18 **"Records"** means all documents and Records housing data, including held, created, used or Processed by the Agency, including Records containing Personal Information.

2.19 **"Transfer Agreement"** means the agreement that governs the relationship between a Responsible Party and a person or entity who receives Personal Information from the Agency who is situated outside South Africa.

3. SCOPE AND APPLICATION

This Policy applies to any person who Process Personal Information on behalf of the Agency as Operators.

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. To discharge the above obligations, the Agency 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 his, her or its Personal Information where there is a lawful basis for such Processing. A lawful basis for Processing Personal Information in terms of POPIA 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 to **comply with a law** or to comply with certain legal obligations imposed by law;
- the Processing is necessary to **protect the Agency'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 which overrides those legitimate interests;
- the Processing is necessary to perform a **public duty** or 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, the Data Subject, has to Consent to the Processing.

5.3 Personnel must ensure that before 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 Agency 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 his / her, Consent so long as it provides the Agency with a "withdrawal of Consent notice", referenced as Schedule 1, which notice is available on the Agency website, which request will be handled and actioned directly by the duly appointed Agency Information Officer , which outcome, in turn, 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 Agency 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" , referenced as Schedule 2, is sent to the Agency, which notice is available on the Agency website, which request will be handled and actioned directly by the 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 the Processing, the Agency and the respective Personnel who has been Processing the impacted Personal Information, will have to stop Processing the Personal Information, unless the Agency 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 At the time of the withdrawal or objection referred to above, the Information Officer will 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 Agency for the Purpose of carrying out its business and related objectives will Process 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 - laws;
- dealing with regulators - laws;
- paying taxes - laws;
- collecting debts or legal proceedings - legitimate interest;
- communications - legitimate interest;
- managing employees - employment.

6.4 Agency 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 is described under the Agency Processing Notices, housed on the Agency website, which the Data Subject should be directed to.

7. ACCURACY

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

7.2 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 which they Process is correct, having regard to the Purposes for which it is Processed, and where it is found to be inaccurate, without delay that is where possible, update and rectify the incorrect Processing of Personal Information;
- implement procedures allowing Data Subjects to update their Personal Information;
- send out regular communications to Data Subjects requesting "updates to details" which, if responded to, should be acted on immediately by the relevant or responsible Personnel;
- 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 concerning these updates and rectifications of Personal Information, housed under the Agency Processing Notices, and give effect to any update request when such request has been communicated to it by the Information Officer.

8. DATA MINIMISATION

8.1 The Agency 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 Agency, that it is adequate, relevant, and limited to what is necessary for the Purposes for which it is Processed; and
- revisit all pre-populated questionnaires and forms which are currently used to collect or house 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 Agency has a duty to show that it has dealt with a Data Subject in a transparent manner.

9.2 To demonstrate transparency, the Agency must refer all Data Subjects, to a specific and informed Processing Notice, at the time when the Agency collects and Processes a Data Subject's Personal Information or within a reasonable period after that, 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 borders 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 To meet its obligations under 9.2 above, the Agency has developed and place on its website the following informed and specific Processing Notices which apply to the different Data Subject categories with whom it deals with:

- a **Human Resources Processing Notice,** which applies to all employees – perspective and actual, all bursary or learnership beneficiaries - prospective or actual;
- an **Infrastructure Procurement Processing Notice**, which applies to all participants in the Agency supply chain and units, including persons who provide goods and services to the Agency (service providers), persons or entities who purchase goods or services from Agency (customers), and/or other parties who the Agency may engage with and who make up the Agency's procurement and supply chain, including Regulators;
- A **Secretarial Processing Notice** which applies to all Data Subjects who deal with the Agency from a secretarial perspective;
- a **Security Processing Notice**, which applies to any persons who come onto the Agency's sites, facilities, and offices and who the Agency may engage with;

- a **Website Privacy Notice** which applies to any persons who use the Agency's websites, social media websites, emails, and other IT-related communications facilities and platforms.

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

- must understand the provisions of the Agency Processing Notices;
- familiarise themselves with the abovementioned Agency Processing Notices and any others which the Agency may implement from time to time, and any changes made thereto;
- familiarise themselves with, where applicable, the Agency's standard binding policies, its standard Personal Information Transfer Agreement and/or its Operator Agreement;
- ensure that all Agency Records that house or call for Personal Information contains the following Processing Notices details:

"In order for the Agency to engage with you, it will have to Process certain Personal Information which belongs to you, which Processing is described and explained under the specific and informative Agency Processing Notices, housed for ease of reference on the Agency website which we ask that you download and read. By providing us with the required Personal Information, such act will be taken to indicate that you have read and agree with the provisions described under the Agency Processing Notice(s), and where applicable, you Consent to the Processing by us of your Personal Information"

- at the time of Processing, direct the Data Subjects you deal with to the applicable area of the Agency website where the specific and informative Agency Processing Notices are housed.

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

10.1 To safeguard, secure, and ensure the confidentiality and integrity of all Personal Information held by or under the control of the Agency, the Agency 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 of 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 these 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 housed within the Agency environment;

  - applications and Processes which has 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 standard Information Technology (IT) Security Audits.

10.2 The duty to ensure data privacy, confidentiality, and integrity of Personal Information start when the Agency 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 Tio ensure the confidentiality and integrity of all Records, especially those which houses or contain Personal Information which the Agency holds, and 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 housed in a folder (Folder), and where applicable in subfolders 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 Agency naming convention, and classification guide and template set out under **Annexure "A"**;

11.1.3 Folders and Records must be named consistently and logically 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 Agency 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 the Agency's specific Records register which has to be compiled for each unit, using the Agency standard department management register (hereinafter referred to as **"the GIFA's File Plan"** read together with the Agency "Records Management Policy **Records**, 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 available.

11.1.6 their respective unit annual head reviews to their own unit specific Records management register to ensure compliance with this Policy;

11.1.7 each unit provides a copy of its 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 Agency Folders or Records is removed immediately and that all Agency assets used to access the Folders and or Records are returned to the Agency, and that all physical access rights to the Agency premises and facilities are revoked or cancelled.

12. RECORDS MANAGEMENT DUTIES: STORAGE OF RECORDS HOUSING PERSONAL INFORMATION

12.1 To ensure the confidentiality and integrity of all paper-based Records that house or contain Personal Information, which are held by the Agency, and 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 File Plan;
- 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 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 Agency's premises if such removal is recorded in the 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 which house or contain Personal Information, which the Agency holds, and to safeguard and secure these Records, Personnel must ensure that:

- they comply with all applicable Agency IT Policies and Procedures, especially the Agency IT End-User policy, referenced as Schedule 3 on the GIFA website;

- all electronic Records are stored and housed on Agency's servers which are protected by the approved security software, and one or more firewalls under the direction of the Agency's IT manager and where transferred or uploaded to cloud computing services from computers, devices and applications, that the Agency IT manager has approved these services;

- all devices where electronic Folders and/ or Records are stored are password protected and passwords are not written down or shared, irrespective of seniority or status of the unit , 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: smartphones, tablets, and Ipads, digital media, Universal Serial Bus (USB) sticks, external hard drives, Compact Disks (CD's), Digital Video Disks' (DVD's), 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 the Agency's secured servers, and which will be downloaded on- to the 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 Agency Records Register and 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 Agency provided systems and applications by following backup protocols. Such backups will be

tested periodically in line with the Agency's standard backup procedures and protocols under the direction of the IT manager;

- all device screens, when not in use, are always locked, especially when left unattended and password protected;

- electronic Records are only transmitted over secure networks, including wireless and wired networks.

12.3 To ensure the confidentiality and integrity of all Records which house or contain Personal Information, which the Agency holds, and 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 and 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 Agency systems and resources, and 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 that 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 (i.e. restricted or confidential) information shall be 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 manager .

12.4 Any attempts to bypass security controls or obtain unauthorised access or make unauthorised use of another's account shall be considered a security breach or violation.

12.5 The use of any Agency information or data for Purposes other than for authorised business Purposes shall be considered a security violation.

12.6 The use of any Agency 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 as 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 Agency 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 Agency for lawful Purposes related to its functions or activities;
- is required by a contract between the parties thereto; or
- is as per Consent received from the Data Subject who owns the Personal Information.

13.2 Records housing Personal Information may be retained indefinitely for business, historical, statistical, or research Purposes provided that the Agency has established appropriate safeguards against the Records being used for any other Purposes.

13.3 Each unit in the Agency 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 needed.

13.4 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 Agency Records Retention Management Policy;
- the record retention periods and related requirements are recorded in the Agency's relevant 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 in 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 unit head must obtain permission to delete or destroy said Folder or Record from the Information Officer / file plan manager, which will be reflected in the relevant department File Plan;

- each unit, once approval for the deletion / destruction of the Folder or Record has been received, via the head of the unit 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 / file plan manger, 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 appropriate Records 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 unit head is responsible for documenting the destruction details under the Agency Records management register.

14. OPERATORS

14.1 Where the Agency makes use of an Operator, in terms of sections 19-21 of POPIA, it must ensure that the Operator only uses the Personal Information as per the mandate to Process Personal Information issued by the Agency, keeps the Personal Information placed under its control, confidential, secure and safe, and that a standard Agency Operator Agreement / Addendum (hereinafter referred to as the "Operator Agreement / Addendum") is concluded between the Agency and the Operator, which 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 Agency, which Operator Agreement / Addendum is housed on the Agency website.

14.2 All Personnel must:

- familiarise themselves with the standard Agency Operator Agreement / Addendum;
- ascertain whom 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 Agency Operator Agreement / Addendum or a similar one which has been approved and vetted by the Agency's compliance unit;
- ensure that an Operator follows the Operator Agreement / Addendum 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 Agency may not share Personal Information with third parties in South Africa, unless:

- there is a legitimate business need to share the Personal Information; or
- the Data Subject has been made aware that his, her, or its 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 Agency Personal Information Transfer Agreement, which is housed on the Agency website or were acting as an Operator has concluded an Operator Agreement / Addendum with the Agency, before receipt of the Personal Information.

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 his, her or its Personal Information will be shared with others and has, where required, given Consent to such sharing; or

- in the absence of the above two situations, has signed the standard Agency 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 Agency Operator Agreement / Addendum is concluded with the Operator before receipt of the Personal Information;

- that any requested deviations for the standard Agency Personal Information transfer agreement or the Operator Agreement / Addendum are vetted and approved by the Agency's compliance unit;

- when sending emails that contain Personal Information, that are marked "confidential", but do not contain the Personal Information in the body of the email, whether sent or received, should rather be 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 Agency may not transfer Personal Information to another party who is situated outside South Africa, unless:

- the Data Subject Consents (under POPIA); or
- the transfer is necessary to perform a contract between the Agency 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; or
- the country where the Personal Information is being transferred to provides the Data Subject with the same level of protection as is housed under POPIA, the data processing law applicable in South Africa; or alternatively,
- the Agency has concluded a Personal Information Transfer Agreement with the recipient of the Personal Information, which sets out the rules which apply to the receipt and the subsequent Processing of that Personal Information.

16.2 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 Information Regulator has issued an "adequacy decision" confirming that the territory or country where the Agency 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 Agency Transfer Agreement or Operator Agreement / Addendum has been concluded with the recipient of the Personal Information;
- the Data Subject has given Consent to the proposed transfer, having been fully informed of any potential risks;
- the transfer is necessary to perform a contract between the Agency 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.

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 Agency customers, when approached or dealt with for the first time, are informally given the opportunity to agree or disagree to the receipt of any Agency direct marketing material and that where the 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 his, her, or its Consent thereto, which will be in the form of the prescribed "opt-in" notice;

- when marketing material is sent to Data Subjects, who have "opted-in" that the material houses an "opt-out" form, allowing the Data Subject to opt-out of any further marketing material; and

- when a Data Subject exercises his, her or its right to object to receiving direct marketing, in the form of an opt-out, such opt-out is recorded and given effect to, and no further direct marketing is sent to the opted-out customer.

All Personnel, especially those who engage in direct marketing, must familiarise themselves with the Agency marketing opt-in and opt-out procedures and forms.

18. REPORTING PERSONAL INFORMATION BREACHES

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

18.2 The Agency 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 Agency data breach report, which report format is annexed hereto marked **Annexure B** and which 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;
- 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 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 several rights under POPIA in relation to his, her, or its 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;
- to object to direct marketing;
- be notified of a Personal Information breach; and
- to complain.

19.2 The Agency has developed, implemented, and will maintain certain Processes and related forms that affect these Data Subject rights, which Processes and related forms are contained in the specific and informed Agency Processing Notices which can be found on the Agency website. When a Data Subject is desirous of exercising these rights, then he, she or it must be directed to the Agency website at: https://gifa.co.za/, where the relevant Processing Notices and related prescribed forms are housed, which form, once completed, must be directed to and handled directly by the Information Officer or their deputy, and no other, 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 concerning 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 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 Agency 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 under a law known as the Promotion of Access to Information Act, 2000 (PAIA) and which request procedure is more fully set out under the Agency's PAIA Manual available on the Agency website.
- where asked by any Data Subject to give effect to these rights, do not deal with the request directly but instead direct the Data Subject to the relevant Process and form on the Agency website, and assist in completing the form only.

20. THE RIGHT TO COMPLAIN

20.1 A Data Subject has the right to lodge a complaint regarding the Processing of his, her, or its Personal Information.

20.2 The Agency 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 Agency website, and to submit the complaint, once completed, directly to the Information Officer.

20.4 In 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, in that case a record setting 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 Agency has appointed the below mentioned parties as its Information Officer(s) and Deputy Information Officer(s):

Information Officer:
Mr Potsishi Hendriek Seabi in his capacity as Chief Executive Officer
Tel: 011 290 6600
email: O.Seabi@gifa.co.za

Deputy Information Officer:
Mrs Liesel Lombaard in her capacity as Chief Director PPP & Compliance
Tel: 011 290 6600
email: l.lombaard@gifa.co.za

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 Agency'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 to ensure that appropriate technological and operational measures have been implemented to provide 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 Agency's Human Resource 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 Agency 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 Agency's operations or concerning Agency activities must be taken up with the Information Officer.

21.3 The Agency's IT unit will be responsible for the following:

- conducting cyber-security risk assessments, including base-line risk assessments of all the Agency information technology activities;

- ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place 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 Agency as a whole or a particular part of it, unit, Personnel concerning any aspect of the Agency work, including password protocols, data access protocols, groups 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 Agency 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 to address all IT security risks which may present themselves in respect of these external service providers.

22. TRAINING

22.1 The Agency will conduct regular training sessions covering the contents of the data privacy laws and the Agency 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 to understand the data privacy laws and how they may impact the Agency Personal Information Processing activities;
- familiarise themselves with the Agency's 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 Agency 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.

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

VERSION AND AMENDMENTS

This Policy is effective as of 1st July 2021.

ANNEXURE A

DOCUMENTS AND RECORDS CLASSIFICATION INSTRUCTIONS AND REGISTER FORMATS

CLASSIFICATION INSTRUCTIONS

Any person who collects, uses, stores, or transmits documents ("Documents") and Records has a responsibility to maintain and safeguard such data ("Data")

This Policy must be read together with the Agency's Records Management Policy, and IT End User Policy available on the GIFA website.

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

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

In the context of information security, Documents and Records classification also addresses the impact to the Agency 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 Agency Documents and Records are categorised into one of 4 (four) sensitivity classifications:

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 Agency's operational effectiveness, cause financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence and therefore information integrity is vital.

Examples of these types of Documents and Records include passwords and information on corporate security procedures; know-how used to Process client information; 'Standard Operating Procedures' used in all parts of Agency's operations; all Agency-developed Intellectual Property, whether used internally or in transactions with third parties.

Confidential Documents and Records

Documents and Records should be classified as confidential ("Confidential") when the unauthorised disclosure, alteration, or destruction of Documents and Records could cause a significant level of risk to the Agency.. Examples of Confidential Documents and Records include Documents and Records protected by state 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 the Agency. 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 affiliated to the respective Agency 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 responsible for the Data.

Confidential Documents and Records are highly sensitive and may have personal privacy considerations or may be restricted by state law. In addition, the negative impact on the Agency should these 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; Confidential Documents and Records and Confidential contracts; non-disclosure agreements and any information shared in respect thereof and the Agency's strategic plans.

Records shall be protected in terms of the POPIA by following the Agency's POPIA Policy.

Internal / Private Documents and Records

These type of Documents and Records can be defined as any information that is Proprietary or produced only for use by f the Agency that 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 those Documents and Records could result in a moderate risk to the Agency.. 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 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 the a respective unit/section in the Agency.

Internal / private Documents and Records is moderately sensitive. Often, internal / private Documents and Records are used to make decisions, so it is important that this information must remain timely and accurate. The risk for negative impact on the Agency should this information not be available when needed is typically moderate. Examples of internal / private Documents and Records include official Agency Records such as financial reports, human resources information, some research Data, unofficial employee Records, budget information, internal operating procedures, operational manuals, internal memoranda, emails, reports, 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 Document and Record would result in little or no risk to the Agency. While little or no controls are required to protect the Confidentiality of the public Data, some level of control is necessary 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 Agency, 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 common in Purpose or function. When classifying a collection/group of Data, the most restrictive classification/category of any individual Data elements should be used. For example, suppose 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

Information security aims to protect the Confidentiality, integrity, and availability of information assets and systems. Data classification reflects the level of impact to the Agency if Confidentiality, integrity, or availability of the Data is compromised.

POTENTIAL IMPACT	LOW	MODERATE	HIGH
Security Objective			
Confidentiality - 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.
Integrity - 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.
Availability - 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			
	Proprietary Data	**Confidential**	**Internal / Private Data**	**Public data**
Access Control	Viewing and modification restricted to authorised individuals as needed for business-related roles. Data owners or custodian grants permission for access, plus approval from line manager. Authentication and authorisation required for access. Confidentiality agreement required.	Viewing and modification restricted to authorised individuals as needed for business-related roles. Data owners or custodian grants permission for access, plus approval from line manager. Authentication and authorisation required for access. Confidentiality agreement required.	Viewing and modification restricted to authorised individuals as needed for business-related roles. Data owner or custodian grants permission for access, plus approval from the line manager. Authentication and authorisation required for access.	No restrictions for viewing.
Copying Printing (applies to both paper and electronic)	Data shall only be printed when there is a legitimate need. Copies shall be limited to individuals authorised to access the Data and have signed a Confidentiality agreement. Information shall not be left unattended on a printer / desk. Control access to print output on copier.	Data shall only be printed when there is a legitimate need. Copies shall be limited to individuals authorised to access the Data and have signed a Confidentiality agreement. Information shall not be left unattended on a printer / desk.	Data shall only be printed when there is a legitimate need. Copies shall be limited to individuals on a need-to-know basis. Information shall not be left unattended on a printer / desk. Control access to print output on copier.	No restrictions

	Copies shall be labelled as per categorisation "Confidential" or "Proprietary".	Control access to print output on copier. Copies shall be labelled as per categorisation "Confidential" or "Proprietary".		
Physical Security	**Hardcopy**: Secure in locked cabinet or location with appropriate physical controls. Physical access shall be monitored, logged, and only give to authorised individuals.	**Hardcopy**: Secure in locked cabinet or location with appropriate physical controls. Physical access shall be monitored, logged, only to authorised individuals.	**Hardcopy**: Secure in locked cabinet or location with appropriate physical controls.	System shall be locked or logged out when unattended.
Information storage	Storage on a secure server, cloud **recommended**. Storage in a secure Data centre or cloud **recommended**. 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. Encryption on backup media required. Use restricted access folders. **Mandatory:** File password protection for sensitive files at Document level. Hardcopy: Secure in locked cabinet or location with appropriate physical controls.	Storage on a secure server or cloud **recommended**. Storage in a secure data Centre or cloud **recommended**. Should not store on an individual's workstation, mobile device (cell phones, laptops, iPad, etc.) or removal devices (USB, external hard drives). Hardcopy: Secure in locked cabinet or location with appropriate physical controls. Use restricted access folders. **Mandatory:** Fil password protection for sensitive files at document level.	Storage on a secure server or cloud **recommended**. Storage in a secure data Centre or cloud **recommended.** Lock screen when unattended.	Storage in a secure server recommended. Storage in a secure Data centre. Lock screen when unattended.

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

FILE PLAN

GAUTENG INFRASTRUCTURE FINANCING AGENCY

Effective date: 1st October 2019

1. CLARIFICATION: RESPONSIBILITIES

The Agency ensures that business Records are created, kept, circulated, stored, and archived appropriately. It is the function of the National Archivist to decide whether items/Records have archival value or not. The Agency must preserve archival Records for 20 (twenty) years and copy them as A20 before arrangements can be made to be transferred into an archives repository.
If an item/Record does not have archival value, the Agency must determine the retention periods for these Records and mark them as D + Number of years.
When determining the retention periods of the Agency's Documents, financial accountability, functional needs, and any statutory requirements that these Records must satisfy must be taken into account. A disposal authority must be obtained from the National Archives. Once a disposal authority has been issued, the Agency may dispose of the Records as authorised.

2. REPORTING

All amendments and additions should be submitted regularly to the National Archivist for notification and formal approval. When these amendments/additions are circulated using circular minutes, it will suffice if a copy thereof is forwarded. For easy reference and effective control, the notification should be numbered each year starting at number one, e.g. 1/2013, 2/2013, etc. It is advisable that in cases where major amendments and/or additions are required, the prior approval of the National Archivist should be obtained before covers for the new files are opened.

3. CONTROL OF THE SYSTEMS

Control of the systems is assigned to the Records Manager. No amendments/additions to the File Plan may be made without the approval of this manager.

4. ACCURATE FILING OF CORRESPONDENCE

All officials conducting correspondence should be supplied with a copy of the File Plan. Officials must be conversant with the series they work with and ensure that all correspondence is dealt with on the correct file. Incorrect filing should be rectified immediately to ensure that valuable material is not destroyed and prevent the retention of ephemeral documents.

5. REGISTER OF FILES OPENED

A register of closed D-files should be created as soon as disposal instructions have been obtained. This register is scheduled over the years, e.g. 2008, 2009, 2010, etc. When a volume is closed, the reference number should be entered in the year it will be destroyed.

6. REGISTER OF FILES FOR DESTRUCTION

A register of closed D-files should be created as soon as disposal instructions have been obtained. This register is divided into years, e.g. 2008, 2009, 2010, etc. When a volume is closed, its reference number should be entered under the year it will be destroyed. A volume that is closed in 2008 and for which the disposal instruction is D3 will therefore be entered under the year 2011, thus making it easily apparent which files are to be destroyed in any particular year.

7. OPENING OF FILES AND DESCRIPTION ON FILE COVERS

Files should be opened only when required. Care should be taken that the numbering and description of the files, as indicated in the file plan, are strictly adhered to. If file descriptions are too lengthy, certain components, which do not form an essential part of the heading, may be omitted. Although certain features may be omitted, the title of the MAIN SERIES must always be given, and the heading must be sufficient to describe the contents of the file. The Records Manager should indicate which components may be omitted in such cases to assist the registry staff. Titles should be printed in indelible ink. The dates of the first and last correspondence and applicable disposal instructions, when available, should be indicated on the file cover.

8. DISPOSAL OF FILES

Once the disposal authority has been issued, such instructions are reflected opposite each file in the disposal column provided in the file plan. The disposal symbols indicate the following:

A20 means to keep for eventual transfer to the appropriate archives repository;

D means destroy after the lapse of the number of years marked by the number following the letter D.

Files should be disposed of regularly, but at least once a year. The prescribed disposal certificate should be submitted to the National Archivist. In the case of files not closed but containing correspondence that may be destroyed, such correspondence may be removed and destroyed. The date on the file cover denoting the date of the first document on the file should then be amended accordingly.

9. CLOSURE OF IMPORTANT FILES

The following procedure should be followed when A20 files are closed:

a) Every page of the correspondence should be examined in order to rule out any misfiling. A sheet of paper with the words “Closed – continued in Volume ….” written on it is then filed as the last item in the file cover;

b) Worn files covers should be replaced;

c) The files are then placed and stored in boxes especially used for this purpose.

10. CASE FILES

Case files, which form part of the File Plan are to be opened by following the instructions appearing at the appropriate places in the file plan. For particulars regarding case files, which do not form part of the File Plan, see the LIST OF SERIES OF SEPARATE CASE FILES at the end of the numerical classification.

11. SECRET FILES

Regarding secret files, the following procedure should be followed:

a) Secret files may be opened for any main series, sub-series, or file appearing in the Master Copy of this file plan. These files are distinguished from the ordinary files by the addition of a capital letter S to the existing reference number.
b) Should a secret file be needed for a subject for which a suitable main series, sub-series, or file does not exist, an appropriate heading should be provided and reported to the National Archivist.
c) Secret files are not indicated in the Master Copy and are also not recorded in the Register of files opened for ordinary files. A separate Register of Secret Files should be opened.
d) Separate arrangements for the safekeeping of secret files must be made and should n not be incorporated as a part of these instructions.
e) The disposal instruction for all secret files is A20, and they should be dealt with a accordingly.

12. LIST OF MAIN SERIES

- Legislation
- Organisation and Control
- Human Resource Management
- Financial Management
- Supply Chain Management
- Facilities Management
- Travel and Transport Services
- Information Management
- Communications
- Legal Services
- Attending and Hosting Events and Conferences
- Projects

An example of project development filing below:

12/1/1	**Project Initiation**
12/1/1/1	Letter of request
12/1/1/2	Response letter
12/1/1/3	Project request form & supporting documents (Land acquisition & Pre-feasibility)
12/1/1/4	All other communications (Pertaining to Sourcing & Filtration Criteria)
12/1/2	**Admin**
12/1/2/1	Screening Report & Multi-Criteria Assessment Report
12/1/2/2	PPF submission
12/1/2/3	PPF approval and conditions
12/1/2/4	Draft MoU
12/1/2/5	ToR (BSC/Probity Approval)
12/1/2/6	Approved MoUs/SLA
12/1/2/7	Signed TA Contract
12/1/2/8	BSC Submission & BSC Approval
12/1/2/9	BAC Submission & BAC Approval
12/1/2/10	Tender Award Letter/Purchase Order
12/1/2/11	TA Tender Advert
12/1/2/12	Workshops (Presentation, Attendance Register, Minutes & Agenda)
12/1/3	**Feasibility Study**
12/1/3/1	Appointment of PSC by CEO: GIFA/Client Department or Municipality
12/1/3/2	Project charter
12/1/3/3	PSC minutes
12/1/3/4	Feasibility report per deliverable.
12/1/3/5	Full feasibility study
12/1/3/6	Project Appraisal Report (PAR)

12/1/3/7	60 Days Public Participation
12/1/3/8	Provincial Exco or Council Approval
12/1/3/9	TAI/TVR1 application (including GPT or Municipal Funding Support letter)
12/1/3/10	TA1/TVR1 Approval with or without conditions & response
12/1/3/11	Draft RFQ/RFP
12/1/3/12	FS Communication sub-folder

12/1/4	**Market Release**
12/1/4/1	Market Sounding Report (Market Testing)
12/1/4/2	TA2A / TVR2A Submission to NT
12/1/4/3	TA2A / TVR2A approval from NT
12/1/4/4	RFQ/RFP to market
12/1/4/5	RFQ/RFP Tender Advert
12/1/4/6	Draft PPP agreement
12/1/4/7	TA2B /TVR2B application
12/1/4/8	TV2B/TVR2B Approval
12/1/4/9	Negotiations with Preferred Bidder
12/1/4/10	60 Day Public Participation

12/1/5	**Financial Close**
12/1/5/1	Subsidiary agreement
12/1/5/2	Shareholder agreement
12/1/5/3	Loan agreement
12/1/5/4	EPC
12/1/5/5	TA3/TVR3 application
12/1/5/6	TA3/TVR3 Approval
12/1/5/7	Council Resolution/Provincial Exco Approval
12/1/5/8	Signed PPP agreement
12/1/5/9	Communication sub-folder

The complete File Plan is obtainable from the Agency Website.

The Records maintained by the Agency were reviewed on the 30th June 2021

ANNEXURE B

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 obtain clarification when in doubt.

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

INCIDENT SUMMARY (SHORT STATEMENT OF EVENT)

INCIDENT INVESTIGATION

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

WHO WAS INVOLVED?

WITNESSES?

WHAT HAPPENED?

WHEN DID THE INCIDENT OCCUR?

WHERE DID THE INCIDENT OCCUR?

THE EXISTENCE OR LOCATION OF ANY PROOF THAT MAY EXIST?

EXTENT OR CONSEQUENCES OF THE DAMAGE / COMPROMISE ETC

Consequences of incidents: Those found in breach of this Policy and any associated procedures and guidelines may result in disciplinary actions up to and including dismissal. Legal and criminal actions may also be penalties to individuals who intentionally obtain or disclose protected information without authorization.

Signature: _____

Date: _____

End