DATA PRIVACY AND INFORMATION SECURITY POLICY

TABLE OF CONTENTS

======//======

DATA PRIVACY AND INFORMATION SECURITY

A. Definitions-Data Privacy and Information Security

Data Privacy is the rights and obligations of individuals and organisations with respect to the fair and lawful collection, use, retention and disclosure of personal information.

Information Security is the protecting measures implemented by an organisation to protect the integrity of such data and information within that organisation from a wide range of threats in order to adhere to applicable legislation and to ensure business continuity, minimise business risk and maximise returns on investment.

B. Preamble

Data Privacy and **Information Security** is an integral component of the Information Management structure of **GEOFFREY SUTHERNS ATTORNEYS**, hereinafter referred to as the **"Firm"**.
The Firm's underwriting of the general governing principles of Data Privacy will also be contained in a **Data Privacy Policy** and an official Firm **Data Privacy Statement** that will be made visible to all interested parties at its operational premises and Web Site as may be appropriate.

The Firm also has an obligation to ensure appropriate security for all Information (IT) systems (data, equipment and processes) and personal information that it owns and/or controls on behalf of other responsible parties, which will be underwritten in an **Information Security Policy.**

Appropriate levels of security will be determined by risk assessment, i.e assessment of threats to, impacts on and vulnerabilities of IT systems and information and the likelihood of their occurrence.

The need for data privacy and information security is driven by the following:-

- Legal, statutory, regulatory and contractual obligations;
- Risk assessment;
- Operational principles, objectives and requirements for information systems that the Firm has defined or developed.

Compliance approach

The Firm will primarily apply a ***"risk based approach"*** to its compliance initiatives in order to mitigate all known and foreseeable risks in addition to any statutory compliance requirements and will combine the Data Privacy Policy and Information Security Policy into one comprehensive document together with other directly related

policies as a result of the close relationship between the two concepts, as well as the practical implementation of the requirements thereof.

C. Management intent

Against the background of the aforementioned, it is therefore the focused intent of the Firm to incorporate all the applicable principles and controls in this policy in order to preserve the constitutional right to privacy and the subsequent protection of personal information in compliance with the requirements of governing legislation and to monitor and enforce compliance to its prescriptions by way of establishing the necessary controls, mandated management, reporting and disciplinary structures to facilitate these outcomes.

D. Objectives

In order to create effective and visible guidelines for the Firm, its employees and any associated third party alliances or subcontractors, this combined policy has been specifically designed to meet the required compliance standards regarding the following aspects:

- Management of information security and data privacy within the structure of the Firm;
- To manage and maintain the security of information and data processing facilities that are accessed, processed, communicated to, or managed by external parties;
- To ensure that all data and personal information receives an appropriate level of protection;
- To ensure that employees, contractors and third party users of the Firm understand their responsibilities and are suitable for the roles they perform, or are considered for and to reduce the risk of theft, fraud or misuse of facilities;
- To ensure that employees, contractors and third party users of the Firm are aware of personal information and data security, security threats and concerns, their responsibilities and liabilities and are equipped to support the organisational Data Privacy and Information Security policy of the Firm in the course of their normal work and to reduce the risk of human error;
- To ensure that employees, contractors and third party users of the Firm exit the employment or change employment in an orderly manner;
- To prevent unauthorised physical access and damage to, or interference with the premises, data or personal information related to the Firm;
- To ensure the correct and secure operation of all data and information processing facilities within the Firm;
- To implement and maintain the appropriate level of data and information security and service delivery agreements;
- To minimise the risk of system failures;
- To protect the integrity of software data and personal information;

- To maintain the integrity and availability of back-up of data, information and related processing facilities;
- To ensure the protection of data and personal information in any networks related to the Firm, as well as protection of the supporting infrastructure;
- To prevent unauthorised disclosure, modification, removal or destruction of removable assets and media under the control of the Firm ;
- To ensure the security of electronic commerce services (where applicable) and their secure use within the Firm;
- To detect unauthorised data and information processing activities within the Firm;
- To ensure proper, authorised user access and to prevent unauthorised access and the compromise or theft of data and information of the Firm;
- To prevent unauthorised user access and the compromise or theft of personal information or data from data / information processing facilities related to the operations and functions of the Firm;
- To prevent unauthorised access to networked services if and when applicable;
- To prevent unauthorised access to the Firm operating systems;
- To prevent unauthorised access to data and personal information held in any application systems within the Firm;
- To ensure data and information security if and when mobile computing and teleworking facilities are employed by the Firm;
- To ensure that security is an integral part of all relevant data and information systems in use by the Firm;
- To prevent errors, loss, unauthorised modification or misuse of data and personal information in applications within the Firm;
- To protect the confidentiality, authenticity or integrity of data and personal information within the Firm by effective cryptographic means when required;
- To ensure the security of system files;
- To maintain the security of application software, data and information within the Firm;
- To reduce risks resulting from exploitation of published technical vulnerabilities;
- To ensure that any breach in information and data security events and weaknesses associated with information systems within the Firm are communicated in a manner allowing timely corrective action to be taken;
- To counteract interruptions to business activities and to protect critical business processes within the Firm from the effects of major failures of data and information systems or disasters and to ensure their timely resumption by way of a properly implemented Business Continuity and Disaster recovery Plan;
- To avoid violations of any law, statutory, regulatory or contractual obligations and of any security requirements;
- To ensure compliance of systems used by the Firm within its organisational security policies and standards and
- To maximise the effectiveness of, and to minimise interference to or from any information and data systems audit processes.

E. Management subscription

The management of the Firm subscribes to the goals and principles of **Data Privacy** and **Information Security** in line with relevant legislation and its business strategy and objectives.

The relationship of the Firm with its personnel, clients and associates is based on mutual integrity and trust and it is therefore committed to maintaining this trust by protecting the privacy and security of personal information and data disclosed and received from any data subject or data owner at all times and to the best of its ability.

As part of this commitment, the Firm will subscribe in all relevant respects to the following:-

- Protection of Personal Information Act No.4 of 2013;
- Promotion of Access to Information Act 2000;
- Applicable guidelines and controls as per the SA National Standard (ISO/SANS 27001/2 & 22301);
- Generally Accepted Privacy Principles (G.A.P.P), consisting of the following:-

1) ***Management*** - the Firm defines documents, communicates and assigns accountability for its privacy policies and procedures;
2) ***Notice*** – the Firm provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed;
3) ***Choice and Consent*** - the Firm describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information;
4) ***Collection*** - the Firm collects personal information only for the purposes identified in the notice;
5) ***Use and Retention*** - the Firm limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent and retains the information for only as long as necessary to fulfill the stated purposes
6) ***Access*** - the Firm provides individuals with convenient access to their personal information for review and updates;
7) ***Disclosure (to third parties)*** - the Firm discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual;
8) ***Security (for privacy)*** - the Firm protects personal information against unauthorised access (both physical and logical);
9) ***Quality*** - the Firm maintains accurate, complete and relevant personal information for the purposes identified in the notice;
10) ***Monitoring and Enforcement*** - the Firm monitors compliance with its Data Privacy and Information Security policy and procedures and has procedures to address privacy-related complaints disputes and transgressions.

F. Policy application

This policy will apply to:-

- ***GEOFFREY SUTHERNS ATTORNEYS*** (the **"Firm"**);
- Any joint ventures, and/or other business organisations that are owned or controlled by the Firm who receive or process personal information for, or on behalf of the Firm;
- The employees and independent contractors of the Firm;
- Personal information of external data subjects and data owners processed and/or stored by the Firm, as well as the personal information of Firm personnel.

G. Terms and definitions

- **Act (**the) – means for purposes of this document the Protection of Personal Act No.4 of 2013;
- **Asset** – anything that has value to the organisation;
- **Biometrics** – means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
- **Consent** – means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
- **Control** – means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature (**note**: Control is also used as a synonym for safeguard or counter measure);
- **Data Controller** – a mandated individual who decides on the manner and purpose for which personal information is processed;
- **Data owner** – means for purposes of this document the owner of personal information or data obtained by implicit or explicit consent of an individual (i.e. banking institutions);
- **Data Privacy** – means for purposes of this document the act of securing personal data within an organisation by following good practice security procedures and implementing controls in order to confirm that personal data is secure;
- **Data Subject** – the person or persons about whom personal information is collected, stored or processed;
- **Disclosure** – in general terms personal information is disclosed when it is released to parties outside the organisation. (It does not include giving individuals information about themselves);
- **Guideline** – a description that clarifies what should be done and how, to achieve the objectives set out in policies;
- **IMC** – for purposes of this document, refers to the Information Management Committee of a private body;
- **Information Management Committee** – means for purposes of this document a decision making structure in a private body to control, regulate and enforce Information Security policy requirements;

- **Information Officer (Chief)** – (of a private body) means for purposes of this document the head or duly authorised person of a private body as contemplated in sec.1 of the Promotion of Access to Information Act 2000 and s 1 of the Protection of Personal Information Act 4 of 2013 ("the Act") and onto which the duties and responsibilities in terms of s55(1) of the Act are conferred;
- **Information Officer (Deputy)** – (of a private body) means for purposes of this document a person duly designated in terms of s 56 of the Act in order to assist the Chief Information Officer to perform its duties and responsibilities as set out in s 55(1) of the Act and onto which any necessary duties, responsibilities and powers are conferred in order to execute the performance of the duties and responsibilities described in s55(1) of the Act;
- **Information processing facilities** – any information processing system, service or infrastructure, or the physical locations housing them;
- **Information security** – preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved;
- **Information security event** – means an identified occurrence of a system, service or network that is indicating a possible breach of information security policy prescription, or failure of safeguards, or a previously unknown situation that may be security relevant;
- **Information security incident** – an information security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security;
- **Legal Entity** – for purposes of this document, the term legal entity is applied to any organisation within the same ownership chain as an organisation who processes a data owners' personal information and may include joint ventures (consolidated or unconsolidated), parent companies or any other organisation contracted by the data owner. All direct legal entities are required to adhere to the data owners' requirements for data privacy and information security;
- **Media** – any means of containment of data and information by way of, i.e. written documentation, CD, DVD, audio, visual recording, computerised filing, etc. – in context also referring to public news reporting entities, i.e. news papers, radio and television reporters or representatives;
- **Personal Information** – for purposes of this document and in line with the Act, personal information means information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person, including, but not limited to:-

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

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

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

  d) the biometric information of the person;

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

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g) the views or opinions of another individual about the person; and
h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

[**NB**: All of the above is inclusive of information related to next of kin and information that is recorded in electronic formats (*e.g*. in databases, Word documents, Excel spreadsheets, E-mail, CCTV and voice recordings, etc.) and all information about the person recorded in structured hard copy filing systems (*e.g*. Personnel files).];

- **Policy** – overall intention and direction as formally expressed by management;
- **Processing/Data Processing** –any operation or set of operations which is performed upon personal information, whether or not by automatic means, such as collection, recording, organising, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
- **Production Data** – data that is used and/or produced during the normal day-to-day operations in the organisation;
- **Regulator** –means the Information Regulator to be established in terms of sec.39 of the Protection of Personal Information Act;
- **Responsible party** – means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;
- **Risk** – combination of the probability of an event and its consequence;
- **Risk analysis** – systematic use of information to identify sources and to estimate the risk;
- **Risk assessment** – overall process of risk analysis and risk evaluation;
- **Risk evaluation** – process of comparing the estimated risk against given risk criteria to determine the significance of the risk;
- **Risk management** – coordinated activities to direct and control an organisation with regard to risk (**note:** risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication);
- **Risk treatment** – process of selection and implementation of measures to modify, mitigate and reduce risk;
- **Sanitation** – means for purposes of this document, the process of removing all traces of a data subject's or owner's personal information from hard drives and other data storage media, before such equipment is exchanged, sold, discarded, passed to a new user or used for non- Firm purposes;
- **Test Data** – data that is specifically recorded for test purposes and is not used for day-to-day operations within the organisation;
- **Third party/Subcontractor/Operator** – any entity, whether an individual or a company, who is not part of a responsible party's organisational structure, but works
- with the responsible party, or processes personal information of the responsible party under authority of and on the responsible party's behalf;
- **Threat** – a potential cause of an unwanted incident, which may result in harm to a system or organisation;

- **Vulnerability** – a weakness of an asset or group of assets that can be exploited by one or more threats.

H. Related legislation, principles, standards, policies and agreements

- Protection of Personal Information Act 4 of 2013;
- Promotion of Access to Information Act. 2000;
- Prevention and Combating of Corrupt Activities Act 12/2004;
- Companies Act No 7 of 2008;
- King III/IV Code of Governance Principles;
- Generally Accepted Privacy Principles (G.A.P.P);
- ISO/IEC 38500;
- ISO/SANS 27001/2;
- ISO 22301;
- Business Continuation and Disaster Recovery Plan;
- Personnel Policy and Disciplinary Code;
- Prevention of Fraud and Corruption Policy
- E-mail Policy and procedures;
- Acceptable Use Policy and procedures;
- Third Party management Policy;
- Mobile Device Policy;
- Data Breach event reports and protocols;
- Confidentiality agreements: Employees, Third Parties and Contractors;
- Protection of Personal Information Agreements: Employees, Third Parties and Contractors;
- Confidentiality and Non- Disclosure agreements;
- Third Party Service- and Service Level Agreements.

I. Revision of the policy

The general policy will be reviewed on an annual basis to address any changes in the technical domain, or applicable legislation.

In the event of any critical interim developments regarding the above, immediate revision and adaption will be implemented as soon as reasonably possible and the revised documentation circulated and explained to all relevant parties through the Firm's awareness programs and/or information communication channels.

The revision history index of the Policy will then also be updated accordingly.

J. Management control and enforcement

Information Officer and Deputy Information Officers

In order to comply with legislation and to facilitate and manage the outcomes of the declared intent of the management of the Firm regarding this policy, the Chief Information Officer *(hereafter also referred to as **CIO**)* for the Firm will be the **Chief Executive Officer/Senior Partner** or a **duly authorised person** of the Firm according to the requirements as defined under ***Sec. 1 of the Protection of Personal Information Act No.4 of 2013*** and read together with the prescriptions of ***Sec.1 of the Promotion of Access to Information Act 2000***.

The Chief Information Officer will be duly registered with the Information Regulator as is required by the applicable legislation after its establishment and will report to the Senior Management of the Firm as may be applicable.

The Firm CIO will also designate **Deputy Information Officers** *(hereafter also referred to as **DIO's**)* to support the CIO as described under ***Sec. 56 of the Protection of Personal Information Act No.4 of 2013***, read together with the prescriptions of ***Sec. 17 of the Promotion of Access to Information Act 2000*** if and when necessary.
The DIO's will also be duly registered with the Information Regulator after establishment as is required, reporting directly to the CIO of the Firm and will in conjunction with the CIO and any other designated individuals constitute the official Information Management Committee *(hereafter also referred to as the **IMC**)* of the Firm, which will be structured as per an authorised organogram (**Refer Appendix O annexed hereto**) for reporting purposes and communicated as such to all Firm employees and other relevant parties.

The role and responsibilities of the CIO and by delegation also the DIO/(s), will be included in a formalised and documented job description for assessment and regulatory purposes and also to facilitate compliance to ***Sec. 55 of the Protection of Personal Information Act No.4 of 2013***.

(**Refer Appendix P annexed hereto**).

The officers will perform in their respective capacities immediately after appointment, but will officially only take up their duties in terms of this Act after the establishment of the Information Regulator and their subsequent registration with the Regulator.

Breach of Information Security Event

Definition

A breach of Information Security Event can be defined as ***"The actual or potential loss of personal data and/or any information that could lead to identity fraud or have any other significant impacts on individuals or the Firm"***

Application

The prescriptions applicable to this matter will apply to all Firm personnel and third party service providers under contract to the Firm.

Identification of events/incidents

The following are common examples of events, which includes, but is not limited to:-

- Loss or damage to paper based files containing classified or personal identifiable information;
- Loss of computer equipment due to crime or an individual's carelessness;
- Loss of unencrypted computer media e.g. CD, data stick, laptop or other portable device;
- Corrupted data;
- Access to inappropriate websites in breach of policy;
- Theft;
- Fraud;
- A computer virus;
- Successful hacking attack;
- Accessing a system or computer using someone else's authorisation code, either fraudulently or by accident;
- Forced entry gained to a secure room/building housing classified information;
- Finding classified or confidential Firm information outside Firm premises;
- Finding Firm paper or electronic records about identifiable individuals in any location outside of the Firm premises;
- Discussing personnel or any other data subject's personal information with someone else in an open area where the conversation can be overheard by outsiders;
- Personal identifiable information sent by insecure means/lost in transit (*e.g.* pay slips, HR records, financial statements, copies of i/d documents, etc.);
- Unauthorised copying of, or removal of personal identifiable information;
- A fax, e-mail or paper document with personal identifiable information sent to the incorrect recipient;
- Evidence of tampering/damage to data cabling between server and work stations or cabling not installed to acceptable industry safety standards;
- Unsecured handling of information storage systems/equipment during a period of disaster or serious damage to the housing complex due to *e.g.* fire, flooding, earthquake, sabotage, etc.
- Evidence of unauthorised cameras, monitoring devices, or listening equipment in the information processing facilities;
- Suspicious unaccompanied persons wandering around in information security areas;
- Allowing uncleared and/or un-identified third party I/T or other contractor personnel to work on information security systems of the Firm.
- Evidence of unattended and unsecured information processing workstations not securely logged-off during the absence of the operator;
- Evidence of weak or no appropriate password management/log-on procedures;

- Any violation of related security protocols as prescribed by the Firm Data Privacy and Information Security Policy that can possibly lead to the loss of classified information.

Reporting process

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Firm CIO is obliged under ***Sec 22, s/sec 1 of the Protection of Personal Information Act No.4 of 2013*** to notify the Regulator and also (subject to ***s/sec. 3***) the data subject of the event/incident.

Under this policy all Firm employees and third party contractors to the Firm are obligated to report any breach, or suspected breach of information security immediately to the Firm CIO or other designated IMC members via the following prescribed protocol:-

a) The prescribed process for reporting any breach of information security event related to any personal information owned by, or under control of the Firm, will be that any person that has any knowledge or evidence of such an occurrence will be obliged to make an immediate written initial report regarding the incident directly after acquiring the knowledge or evidence of the incident to the CIO, or in his/her absence, to any of the DIO's or other members of the Firm Information Management Committee (IMC);

b) A compulsory **Breach of Information Security Event Report** (*Annexure Q annexed hereto*) must be fully completed by the person witnessing or discovering the incident immediately after the initial report and submitted to the CIO, or in his/her absence, to any of the DIO's or other members of the IMC;

(***NB*** *- **A signed copy of this report must be retained as receipt by the person that submits the report**.*)

c) Only the Firm IMC will be mandated to make a factual assessment of the incident in order to take whatever remedial steps necessary to contain the situation and also for the regulatory reporting of the incident to the Information Regulator, data subject and data owner where it is deemed to be appropriate and applicable;

d) No other employee or any third party contractor of the Firm will have any mandate to decide on the merits, or applicability of any reports in this category, unless specifically authorised to this effect in writing by the CIO of the Firm.

NB - Any violation of this prescription will be addressed via the Disciplinary Code, or the Third Party Management prescriptions of the Firm as may be applicable.

Accountability

Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or non-compliance to the Firm's policy prescriptions, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of the Firm.

The contractual agreements of external third party contractors to the Firm will be subject to immediate suspension or termination in the sole discretion of the senior management of the Firm, pending investigation and recommendations of the IMC of the Firm.

In the event of a monetary loss to the Firm as a direct result of the occurrence of the breach in Information Security, the accountable party, or parties in both instances may be held fully liable for the loss and any costs for recovery thereof in the sole discretion of the senior management of the Firm.

Enforcement criteria

The severity of any disciplinary or other enforcement action taken by the Firm will vary based on factors considered relevant by the IMC, including but not limited to:-

- The sensitivity of the personal data disclosed or used in violation of this policy;
- The number of parties impacted by the violation of this policy;
- The duration of the improper disclosure or unauthorised use;
- Prior improper disclosure or use of personal information by any applicable accountable party;
- Whether the violation or neglect was inadvertent or the result of inadequate training, or supervision.

NOTE: Where the Information Management Committee (IMC) believes that the conduct may constitute a violation of any other applicable law, rule, or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

K. Third Party Management

Where any external third parties are engaged by the Firm for services related to the Firm information systems, processing of personal information within the control of the Firm, or where such parties may have any access to aforementioned information, the relationship with and the performance of such parties will be governed by this policy.

Third Party Operators that may obtain, process or store personal information under authority and on behalf of the Firm as is described under Sec. 20 of the Act, will be subject to a written contract, inclusive of the right to audit the compliance status of

such Operator, with regards to the security measures under Sec. 19 as is required by Sec. 21 of the Act without exception.

The Firm may also engage the services of outside sources when deemed necessary to undertake the necessary audits and inspections if internal resources are not available to perform this task.

All *Third Party Agreements* with the Firm will make provision for the clauses and conditions necessary for these parties to comply with the information security requirements in terms of this Policy and the remedial procedures to enforce these requirements.

The strict *compliance* of all third parties to the conditions contained in the relevant agreements will be monitored by the CIO or dedicated DIO/(s) of the Firm as part of their job description and any violations reported to the IMC for assessment and remedial actions where appropriate.

In the event of any violations or suspected violations of the conditions of third party agreements, the continued engagement of the services of the particular third party may be suspended immediately in the sole discretion of the CIO, pending a proper investigation into the matter in order to mitigate any contamination or potential threats to the integrity of Firm information.

It will also be a non-negotiable requirement and responsibility of all Firm employees and contracted third parties to immediately report any suspicious actions or violations of policy and contractual conditions by anyone in the operational domain of the Firm to the CIO or any of the IMC members.

Any non compliance herein will be strictly dealt with in terms of the Firm disciplinary processes or other necessary and appropriate remediation measures that may be applicable.

L. Dealing with the public media

Only Senior Management or designated representatives of the Firm will be authorised to make any presentation, comment, statement or direct contact with the public media regarding any matter whatsoever regarding any Information Security incident, client information or any business issues directly related to the organisation and/or its operations.

Any employee, contractor, or associated third party that is found in violation of this ruling will be subjected to the applicable sanctions in accordance with the Firm Disciplinary Code and/or any other related policy governance actions that may be applicable.

M. Data Privacy Policy

Preamble

The Firm recognises the Constitutional privacy rights of all individuals, subject to any applicable legal requirements regarding the privacy of personal information.

The Firm also recognises the importance of client privacy and the sensitivity of the personal information concerning any individual that may be contained on the Firm's information storage systems.

As a practicing legal institution, the Firm has a professional and ethical obligation to keep confidential all information received within an attorney-client relationship, subject to the client's instructions to provide legal services.

The Firm is therefore committed to safeguarding the privacy of all personal information in its possession or under its control concerning any individual as may be required under all current and applicable legislation and to subscribe to all individual Privacy Rights as will be set out according to this Data Privacy Policy.

Scope of the policy

The policy will be effective to cover all permanent and temporary employees, associates, 3rd party contractors and operators, consultants and other external entities of the Firm that may have access to, or gain access to any personal information of data subjects contained on the information systems of the Firm.

Individual Privacy Rights

The Firm will manage personal information in compliance with the Protection of Personal Information Act 4 of 2013 (herein after referred to as the Act) and will also comply in all relevant circumstances with any other Acts that may have reference and application.
All data subjects engaging the services of the Firm must be properly advised of their privacy rights prior to any processing of their personal information is initiated.

Individual Privacy Rights, subject to certain provisions under the aforementioned Act, are summarised as follows:-

a) Data subjects are to be notified that:-
   1) Individual personal information is being collected, or
   2) Individual personal information has been accessed or acquired by an unauthorised person;

b) Data subjects will have the right to:-
   1) Establish whether the Firm is holding any of a subject's personal information and to request access to this information;
   2) Request, where necessary, the correction, destruction or deletion of this information;

3) Object, on reasonable grounds related to a subject's personal situation, to the processing of such subject's personal information;
4) Object to the processing of personal information at any time for purposes of direct marketing;
5) Not have personal information processed for purposes of direct marketing by means of unsolicited electronic communication, subject to certain exceptions;
6) Not be subject, under certain circumstances, to decisions based solely on the basis of the automated processing of personal information intended to provide a profile of the data subject (also referred to as *"profiling"*);
7) Submit a complaint to the Regulator regarding any alleged interference with the protection of personal information, or the determination of an adjudicator;
8) Institute civil proceedings regarding the alleged interference with the protection of the data subject's personal information.

Collection of Personal Information

Personal information will only be collected for the purposes of serving the legal and related needs of data subjects as set out in a written processing notification, in order to:-

- Understand, advise and assist the data subject/s with specific or ongoing legal needs;
- Ensure the recorded information is kept accurate and up-to-date;
- Comply with any legal requirements that may be applicable.

Types of Personal Information that may be collected

Personal information as defined under the Act is any information that identifies a data subject and may include the following:-

- Information relating to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth;
- Information relating to education, or medical, financial, criminal or employment history;
- Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to a data subject;
- Biometric information;
- Personal opinions, views or preferences of a data subject;
- Correspondence sent by a data subject that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;
- The views and opinions of another person about a data subject;
- Name, if it appears with other personal information related to a data subject, or if the disclosure of the name itself will reveal information about the data subject.

The Firm will follow reasonable and prudent business practices to legally collect, use and disclose a data subject's personal information only for the purpose of providing the data subject with any required legal services and will not collect any personal

information without the data subject's consent, or that may be excessive to the purpose that it is required for.

Collection process when processing of Personal Information

The Firm's collection procedures will be guided by the following:-

- Collection of personal information will only be by lawful and fair means;
- Directed individual requests for a data subject's relevant sensitive personal information from a particular organisation or business, such as medical professionals or financial institutions, will only be made after obtaining the written consent thereto from the data subject;
- Wherever possible, personal information will only be collected directly from a data subject;
- Data subject's consent will be required at the start of a retainer, or during the course of representation procedures if prior consent was not already obtained;
- Consent will primarily be required in writing, but verbal or implied consent may be accepted as may be necessary to further a data subject's legal needs;
- A Firm Privacy Statement will be published on the Firm website and will also serve as a supportive notice of the purposes for which the Firm collect, use or disclose a data subject's personal information or business contact information;
- Dependent on the legal services provided, with a data subject's consent, the Firm may obtain this relevant information from whatever resource necessary and applicable, including, but not limited to:-
    - The data subject personally;
    - Medical professionals;
    - Public registries such as the Deeds Office, Department of Home Affairs, Receiver of Revenue, or whichever registry may be of essence;
    - Financial institutions (for example to verify financial information);
    - Credit bureaux;
    - Data subject's employer (for example, employment evidence for confirmation of income, etc.);
    - Motor vehicle and driver licensing authorities;
    - Law enforcement, if relevant;
    - Investigators.

Consent

The Firm's guidelines with regards to consent will be as follows:-

- The Firm's general practice will be to primarily request a data subject's written or alternatively express oral consent, which may be given in person or over the telephone if the data subject's identity can be properly authenticated;
- If a data subject volunteers to provide relevant personal information verbally, in writing, or via the Firm website, it may be assumed that the data subject is also consenting to the collection, use and disclosure of personal information as described in the Firm's Privacy Statement;
- When a data subject initiates contact with the Firm, it may be determined that consent has been implied for the Firm to collect, use and disclose personal information in a reasonable and lawful manner;

- In some situations, the Firm will require express consent in writing, by the provision of a letter, application form, electronic signature, or other document authorising certain activities.

As a basic rule, the Firm will handle all personal information confidentially and will substantiate the legal authority to collect, use and disclose personal information in these aforementioned circumstances if and when required.

Note must however, be taken that there are certain circumstances where the Firm is required or permitted by law, to collect, use and disclose personal information without the data subject's consent.

Personal information of a data subject may only be disclosed without the data subject's consent under written authorisation from the Firm's CIO, or other mandated members of the IMC under certain circumstances, when:-

- the Firm is required or authorised by law to do so, for example if a court issues a subpoena;
- the use of the information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;
- it is necessary to establish or collect any fees owed to the Firm; or
- if the information is already publicly known.

Use or application of data subject's personal information

The Firm's accepted practice will subscribe to the following:-

- Personal information will only be used or applied for the purposes intended, to provide legal advice and services to a data subject and to administer the Firm's legal business incidental to providing legal services, such as client billing;
- With the data subject's permission, the Firm may send further information about the Firm's other legal services, or about new developments in the law, to a data subject – *(**NB:** The data subject may at any time withdraw any prior consent by notifying the Firm accordingly, and the Firm will be committed to terminate any further transmission of information immediately)*;
- The Firm will not disclose or sell any data subject personal information or business contact information to any third party to enable them to market their products and services without express prior written consent from any data subject.

Release of data subject personal information

The Firm will only release personal information of a data subject to serve specific needs of the data subject, in the course of providing required legal services.

With the data subject's consent, the Firm may provide information to:-

- Firm staff and agents who use the information for the reasonable business purpose of providing the data subject with required legal services;

- A third party contracted to provide administrative services to the Firm (e.g Correspondents, computer back-up services or archival file storage) on condition that the third party has agreed to comply with the Firm's Data Privacy and Information Security policy requirements and any other applicable privacy laws;
- Professionals employed by the Firm, such as investigators, paralegals and experts;
- Financial institutions, (i.e, the institution that carries a data subject's mortgage loan).

Accuracy of information

The Firm will endeavour at all times to ensure the accuracy and relevance of any personal information on its information systems, while a data subject will have the right to request access and make any necessary correction of own personal information that is held on the Firm information systems.

It will be a basic requirement that a data subject must provide the Firm with accurate and up-to-date personal and business contact information for the purposes of providing the data subject with the required legal services and to maintain contact with the data subject.

If during the course of the professional relationship between the Firm and a data subject, any of the data subject's information should change, it will be required from the data subject to inform the Firm as soon as possible, in order to enable the Firm to make any necessary changes as soon as reasonably possible.

The above requirements must be clearly conveyed to all data subjects entering into a relationship with the Firm at the start of the relationship and put into writing as far as possible to avoid any possible dispute thereof in future.

Protection of personal information

In order to protect all data subject personal information under control of the Firm, the Firm will:-

- Endorse the principles for the processing of personal information as described under the Protection of Personal Information Act 4 of 2013;
- Draft and implement a separate comprehensive Information Security Policy which will include the necessary controls and protocols to mitigate all known and reasonably foreseeable threats to personal information in Firm possession or under Firm control;
- Introduce properly monitored applicable awareness training interventions for Firm employees and where necessary any third party service providers or operators, in order to maximise the safety levels for processing of personal information and minimising the threats of data breaches and loss of personal information;
- Maintain strong management and control protocols over any third-party service providers or contractors with regards to the proper protection and processing of personal information;

- Implement and maintain an effective Information Security Management System (ISMS) with due regard to generally accepted Standards and Principles;
- Not collect, use or disclose personal information for any purpose other than those specified as per prior consent, or which are reasonably evident;
- Only disclose personal information to those persons who have a need to access personal information for the purposes stated in the Firm Privacy Statement or any subsequent notice to process and which will also be specified in the data subject consent to process personal information;
- Keep data subject personal information only for as long as it is needed to fulfill the stated purpose or as may be required by any other applicable, or related legislation;
- Securely and effectively dispose of redundant personal information of data subjects on the Firm's information systems as soon as possible after the fulfillment of the originally stated purposes, unless prohibited by the requirements of any other applicable legislation;
- Maintain data subject personal information in as accurate, complete and up-to-date format as possible;
- Keep all personal information physically secure, (for example, in locked or secure offices, rooms and/or filing cabinets as may be applicable);
- Implement and maintain any reasonably expected and applicable technological safeguards such as passwords or encryption for sensitive personal information on information systems, in storage, in transit, or located on any mobile devices.

Access to personal information

A data subject may request access to own personal information that the Firm may have, or control at any reasonable time.

The request must be in writing and directed to the Firm Chief Information Officer (CIO), or other dedicated Deputy Information Officer (DIO) that will be properly identified and communicated to all interested parties from time to time.

NOTE: It will be an absolute pre-condition that the identity of any data subject requesting access to personal information will be established properly and beyond any reasonable doubt before any access to any personal information will be allowed. *(Also refer to the Firm PAIA Sec.51 Manual for the prescribed process in instances where there are reasonable grounds to refuse access to personal information).*

The Firm may also charge a reasonable fee for retrieval and copying of personal information and if the retrieval or copying or the request from the data subject is extensive, prior notice of such fee must be provided to the data subject prior to retrieval and copying.

Grounds for denial of access to Personal Information

There are exceptions to the data subject's right to access of personal information:-

a) By law, the Firm must deny access when:-

- A data subject's file contains personal information on a third party and the information cannot be severed to maintain the privacy of the third party information;
- Required or authorised by law (for example, when a record containing personal information about a data subject is subject to a claim of legal professional privilege by one of the Firm's clients);

b) The Firm has the right to deny access to personal information and may deny access when a data subject's information relates to existing or anticipated legal proceedings against the data subject, including unpaid bills to the Firm.

In instances where the Firm denies a data subject's request for access to, or refuse a request to correct information, the Firm will issue an explanation and the reason/s for the refusal.

The Firm will however, attempt in all cases to mediate a resolution if possible, but failing this, the data subject must also be advised of the alternative option to revert to the processes as provided for under the Promotion of Access to Information Act (PAIA) and reflected in the Firm Sec.51 PAIA manual that can be accessed on the Firm's website or obtained at the Firm's physical business premises.

Communications by E-mail

The Firm's estimation of this communication medium is that e-mail cannot be regarded as a secure, confidential method of communicating with the Firm with regard to confidential and personal information.

The Firm will not use e-mail to convey personal or confidential information, unless the data subject expressly authorises this form of communication and accepts all the inherent risks associated with this type of communication before any information is conveyed in this manner.

The Firm will draft and implement a specific e-mail policy to also address and manage this aspect properly, the prescriptions of which will have to be followed scrupulously in all respects, even where the data subject consents to this format of communication.

Review of this policy

The Firm will review and change or adapt this policy from time to time in order to update the Firm's privacy commitment to data subjects and in keeping with current privacy laws and changes in the information threat environment.

Any crucial amendments or changes to the policy will be communicated to all interested parties where necessary and the Firm Privacy Statement as published on the Firm website will also be altered accordingly to reflect any changes to the policy.

Non-adherence to the policy requirements

The Firm will enforce adherence to the requirements of this policy in a very strict manner in order to comply with the requirements of the Act and to maximise the protection of the privacy and personal information of data subjects.

Any Firm employee found to be in breach of the policy requirements will be subject to the relevant Disciplinary procedures of the Firm and if any activities related to such breach may be uncovered during these procedures that are also in violation of any other legislation, (*i.e* Anti-Corruption legislation), the Firm will also proceed with criminal charges or other legal processes that may become relevant.

In any instances where third parties or operators under contract to the Firm is found to be involved, or implicated, any further interaction with the affected parties will be suspended immediately pending an investigation into the matter and the contractual conditions contained in the relevant contracts may be invoked and where necessary or applicable, any legal or criminal processes must be initiated as soon as may be reasonably possible.

N. Information Security Policy

Preamble

The Firm is a Responsible Party as defined under the Protection of Personal Information Act No.4 of 2013 and therefore has the obligation to ensure the security of all personal information under its control, whether being processed, conveyed or stored on Firm information systems.

The Firm is also obliged to mitigate the potential negative effects of all known, or reasonably foreseeable risks to the security of all personal information under its control by applying the necessary management controls and policies, whilst also giving due cognisance to all accepted or applicable industry standards, practices and principles.

The Firm also recognises the general principle that ***"there can be security without privacy, but no privacy without security"*** and therefore subscribes to this Information Security Policy also as a fundamental supportive measure to secure the Constitutional right to Privacy as set out in the Firm Data Privacy Policy.

Policy scope

The policy will be effective to cover all permanent and temporary employees, associates, 3rd party contractors and operators, consultants and other external entities of the Firm that may have access to, or gain access to any personal information of data subjects contained on the information systems of the Firm.

The policy will be promulgated to include the following domains and frameworks:-

a) Logical security:
Data security- Inclusive of data privacy principles, confidentiality, criticality, integrity and intellectual property rights;
Communications security- Establishing network connections; Flow control systems inclusive of firewalls, encryption, dial-up communications, telephone systems, electronic mail systems, downloaded data, internet connections and telecommuting arrangements;
Software security- inclusive of system access control and password management; privilege control and logging;
Software development and change control- Inclusive of change control processes for workstations; third party involvement; handling of viruses and worms and software development processes.

b) Physical security:
Physical access security- Inclusive of building and computer facilities access control;
Computer location and environment- Inclusive of premises, emergency data centre premises and their construction, emergency power supply and equipment; alarm systems and contingency planning for emergency situations.

c) Managerial security:
Administrative security- Inclusive of user training and awareness; reporting of security problems and information security breach incidents; controls and risk assessment; outsourcing and third party contracts;
Human Resource- Inclusive of a separate, but consequential Personnel Policy with alignment to relevant Data Privacy and Information Security principles and regulations, background checks, application and appointment procedures, qualifications and skills, Disciplinary Code and Protection of Personal Information agreements;
Business Continuity Management- Inclusive of a separate, but consequential Business Continuation and Disaster Recovery Plan with contingency planning, testing of plans, identification and minimisation of business and Information Security risks.

Review of this policy

The Firm will review and change or adapt this policy annually, or when deemed necessary in the interim in order to maintain legal compliance requirements, update the Firm's security commitment to data subjects and in keeping with changes in current privacy laws, security requirements and the information threat environment.

Any crucial amendments or changes to the policy will immediately be properly communicated to all interested parties where necessary and any other related policies that may be affected by variations will also be altered accordingly to reflect any changes to the policy.

Key controls incorporated in this policy

In order to effect compliance to the requirements set out under Section 19 of the Act, the key controls contained in the ISO 27001 standard will be accepted in a Firm

Statement Of Applicability (S.O.A) for incorporation into this policy and will thereby:-

a) form the basic framework of the Firm's ***Information Security Management System (ISMS)*** and

b) will be applicable as core-controls for implementation, which will be assigned to dedicated members of the IMC as control custodians.

NB: Due recognition of any and all copyrights is also given to the relevant controls and guidance notes contained in the ISO 27001&2 standards that will be used and referred to as annexures in this policy and **no** external copying or publishing thereof for use outside of the Firm will be permissible without prior permission from the ISO Copyright Office.

The Firm will regard eventual full implementation of the ***ISMS*** as absolutely crucial for the maximum enhancement of the effectiveness and execution of the policy, mitigation of known and reasonably foreseeable risks and containment of any violations of statutory compliance requirements by the Firm.

In order to provide a more defined and measurable guidance framework for the ***ISMS*** with regards to the practical implementation of the aforementioned controls, the guidelines as set out in the South African National Standard ISO/SANS 27001&2, ISO 22301, Generally Accepted Privacy Principles (G.A.P.P.) and applicable legal compliance requirements under the Act were integrated and set out according to the following annexures to form part of this policy:-

1) Security information policies **(Annexure A)**;
2) Organisation of information security **(Annexure B)**;
3) Human resources security **(Annexure C)**;
4) Asset management **(Annexure D)**;
5) Access control **(Annexure E)**;
6) Cryptography **(Annexure F)**;
7) Physical and environmental security **(Annexure G)**;
8) Operations security **(Annexure H)**;
9) Communications security **(Annexure I)**;
10) System acquisition, development and maintenance **(Annexure J)**;
11) Supplier relationships **(Annexure K)**;
12) Information security incident management **(Annexure L)**;
13) Information security aspects of B C M **(Annexure M)**;
14) Compliance **(Annexure N)**;
15) IMC -Organogram and Reporting Structure **(Annexure O)**;
16) Information Officer-Job description **(Annexure P)**;
17) Breach of Information Security Event Report **(Annexure Q)**.

=====//=====