Protection of Personal Information (POPI)
CSA GROUP OF COMPANIES
DATA PRIVACY POLICY WEB VERSION

INDEX

1. DEFINITIONS

"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;
"CSA GROUP OF COMPANIES" mean, for purposes of this Policy, the following companies, their employees, shareholders and directors:

"**child**": means a natural person under the age of 18 years who is not competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;
"competent person": means any person who is competent to consent to any action or decision being taken in respect of any matter concerning a child;
"data subject": means the person or entity to whom personal information relates and for the purposes of THE CSA GROUP OF COMPANIES, this will include but not be limited to its clients, its employees, its associates, its service suppliers, industry associates, placements, its directors and any other person or juristic person whose information is collected, processed or shared, whether such person or entity is based in South Africa or abroad;
"direct marketing": means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

- Promoting or offering to supply its services in the ordinary course of business of THE CSA GROUP OF COMPANIES;
- Requesting the data subject to make a donation of any kind for any reason;

"electronic communication": means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"filing system": means any structured set of personal information which in the case of THE CSA GROUP OF COMPANIES consists of physical files kept in the offices of CSA the group together with the data filed on the various software systems used;

"GDPR": means The General Data Protection Regulation 2016/679 which is a EUROPEAN UNION regulation in respect of data protection and privacy in the European Union and the European Economic Area which addresses the transfer of personal data outside the EU and EEA areas and it imposes obligations onto organizations anywhere, if they target or collect data related to personal information from individuals in the EU. The regulation was put into effect on May 25, 2018;

"Information officer": of THE CSA GROUP OF COMPANIES**;**

"operator": means a person or organization who processes personal information for THE CSA GROUP OF COMPANIES who for such purposes will be known as the responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"person": means a natural person or a juristic person;

"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:

- Information relating to the education or the medical, financial, criminal or employment history of the person; Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- The personal opinions, views or preferences of the person;
- Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature;
- The views or opinions of another individual about the person; and
- 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;

"private body": means

- a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
- a partnership which carries or has carried on any trade, business or profession; or
- any former or existing juristic person, but excludes a public body;

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

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distribution or making available in any other form; or
- Merging, linking, as well as restriction, degradation, erasure or destruction of information;

"Promotion of Access to Information Act": means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000);

"public record": means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

"record": means any recorded information regardless of form or medium, including any of the following:

- Writing on any material;
- Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- Book, map, plan, graph, or drawing;
- Photograph, film, negative, tape or other device in which one or more visuals images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; b) In the possession or under the control of a responsible party; and c) Regardless of when it came into existence;

"Regulator": – means the Information Regulator established in terms of Section 39 of the POPIA;

"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;

"restriction": means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"special personal information": means personal information as referred to in Section 26 of the POPIA which includes 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;

"this Act": means the Protection of Personal Information Act, No. 4 of 2013.

"unique identifier": means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2. INTRODUCTION

THE CSA GROUP OF COMPANIES is a talent and brand communication firm that seeks to connect agencies and marketers in a variety of industries and co-ordinate and arrange events. In the fulfillment of its services, THE CSA GROUP OF COMPANIES deal with many role players in the entertainment, sports, talent, brand, marketing, film and communication industries and acknowledge that, in performing its business operations most of its communications are done electronically via the internet and email.

In further recognizing the international risk of data breach and considering the fact that THE CSA GROUP OF COMPANIES is affiliated to an American corporate equivalent, and also to ensure that lawful conditions exist surrounding its international data subject's information, THE CSA GROUP OF COMPANIES are committed to promote the South African Constitutional Right to Privacy and the rights contained within POPIA when dealing with all data subjects' information in South Africa. THE CSA GROUP OF COMPANIES therefore accept that its data subjects based in other parts of the world are entitled to equal rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based and in this regard recognize the need to promote the rights contained in the GDPR when dealing with individual European Union data subjects.

THE CSA GROUP OF COMPANIES are further committed to the education of its data subjects in respect of their rights to privacy and will make all operational amendments necessary.

3. OBJECTIVE

The objective of this Policy is to ensure adherence to the provisions within POPIA, its Regulations, the GDPR and its regulations where applicable aimed at protecting all THE CSA SOUTH AFRICAN GROUP OF COMPANIES's data subjects from harm and in an attempt to achieve this, the group has considered and implemented these rules to protect personal information, to adhere to the requirements of responsible handling of data subjects' information, to ensure that data subjects' Consent is obtained where necessary, to ensure that data subjects' information is not unlawfully shared with third parties unless Consent for such sharing is obtained, and to stop identity fraud.

This Policy constitutes the group's DATA PRIVACY RULES and sets out the standard for suitable protection of personal information as required by POPIA.

4. POPIA CORE PRINCIPLES

In its quest to ensure the protection of data subjects' privacy, THE CSA GROUP OF COMPANIES fully commit as follows:

4.1. To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.

4.2. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

4.3. To ensure that the requirements of the POPIA legislation are upheld within the organization. In terms of sections 8, 17 and 18 of POPIA, THE CSA GROUP OF COMPANIES confirm that it adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribe to a process of accountability and openness throughout its operation.

4.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPI, to undertake to collect personal information in a lawful and reasonable way, for a specific reason and only if it is necessary for operations and to process the personal information obtained from clients and data subjects only for the purpose for which it was obtained in the first place.

4.5. No to process personal information obtained from data subjects in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the data subject.

4.6. In terms of the provisions contained within sections 23 to 25 of POPIA, to allow all data subjects the right to request access to certain personal information and to request correction or deletion of personal information within the specifications of the POPIA and to this end, data subjects are referred to the **FORMS 1 & 2** hereto attached.

4.7. To not request or process information related to race, religion, medical situation, political preference, trade union membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented. THE CSA GROUP OF COMPANIES will also not process information of juveniles.

4.8. In terms of the provisions contained within section 16 of POPIA**,** to record and retain information accurately.

4.9. To not provide any documentation to a third party or service provider without the express consent of the data subject except where it is necessary for the proper execution of the service as expected by the data subject.

4.10. To keep effective record of personal information and undertakes not to retain information for a period longer than specified in the property industry's Code of Conduct.

4.11. In terms of sections 19 to 22 of POPIA, to secure the integrity and confidentiality of personal information in its possession. THE CSA GROUP OF COMPANIES will provide the necessary security of data and keep it in accordance with prescribed legislation.

5. CONSENT

When data subjects' information is collected, processed or shared by THE CSA GROUP OF COMPANIES during the delivery of its services, it recognizes the obligations to explain the reasons for the collection of information from the particular data subject/s and to obtain the required Consents to process and where required the sharing of the information pursuant to such explanation.

When data subjects' information is collected, processed or shared by THE CSA GROUP OF COMPANIES for any other reason than the original reason of it being collected, the specific Consent for such purpose must be obtained from the data subject in addition to the possibility of it having to obtain PRIOR APPROVAL from the Information Regulator in terms of sections 57 and 58 of POPIA.

If SPECIAL PERSONAL INFORMATION is collected, processed, shared and stored for any reason from any of THE CSA GROUP OF COMPANIES's data subjects, specific Consent must first be obtained. The prohibition on collection and processing of special personal information does not apply if:-

5.1. Processing is carried out with the consent of the data subject;
5.2. Processing is necessary for the establishment, exercise or defense of a right or obligation in law;
5.3. Processing is for historical, statistical or research purposes.

THE CSA GROUP OF COMPANIES have amended its standard documentation with references to the Act and will obtain all data subjects' general Consent in order that data subjects are aware at all times of the reasons for the information being collected, how the information will be processed and for what the information will be used.

6. COLLECTION, PROCESSING AND SHARING OF INFORMATION

THE CSA GROUP OF COMPANIES collects and processes personal information from its data subjects for a variety of reasons and in a variety of ways. The most pertinent reason for data collection, processing and sharing of the information relates to the fulfilment of its contractual services and as a result, information is often shared with third parties involved in the project and often cross border with project associates.

The primary way of collection and processing of personal information is electronically. By submitting personal and special personal information details to THE CSA GROUP OF COMPANIES, all data subjects acknowledge that:

6.1. Personal information collected by THE CSA GROUP OF COMPANIES will be collected directly from the data subject, unless –
6.1.1. The information is contained or derived from a public record or has deliberately been made public by the data subject;
6.1.2. Collection of the information from another source would not prejudice a legitimate interest of the data subject;
6.1.3. Collection of the information from another source is necessary -
- 6.1.3.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
- 6.1.3.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
- 6.1.3.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
- 6.1.3.4. In the interest of national security;
- 6.1.3.5. To maintain the legitimate interests of THE CSA GROUP OF COMPANIES or of a third party to whom the information is supplied;
- 6.1.3.6. Compliance would prejudice a lawful purpose of the collection;
- 6.1.3.7. Compliance is not reasonably practicable in the circumstances of the particular case.

6.1.4. Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of THE CSA GROUP OF COMPANIES;
6.2. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.
6.3. THE CSA GROUP OF COMPANIES will take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected and further processed.
6.4. Where personal information is collected form a data subject directly, THE CSA GROUP OF COMPANIES will take reasonably practicable steps to ensure that the data subject is aware of: -
6.4.1. The nature of the information being collected and where the information is not collected from the data subject, the source from which it is collected;
6.4.2. The name and address of THE CSA GROUP OF COMPANIES;
6.4.3. The purpose for which the information is being collected;
6.4.4. Whether or not the supply of the information by the data subject is voluntary or mandatory;
6.4.5. The consequences of failure to provide the information;
6.4.6. Any particular law authorizing or requiring the collection of the information.

7. STORAGE OF INFORMATION

THE CSA GROUP OF COMPANIES acknowledges the risks facing data subjects with the storage of personal and special personal information on THE CSA GROUP OF COMPANIES's software systems as well as filing copies of the physical information sheets containing personal information physically in an office.

To ensure that its best attempts are made to minimize data subjects from suffering loss of personal information, misuse or unauthorized alteration of information, unauthorized access or disclosure of personal information generally, it will:

7.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.
7.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. THE CSA GROUP OF COMPANIES test its systems regularly to ensure that our security mechanisms are up to date.
7.3. Continue to review its internal policies and third party agreements where necessary to ensure that these are also complying with the POPIA and Regulations in line with THE CSA GROUP OF COMPANIES's Policy rules.

8. DISPOSAL OF DATA SUBJECTS' INFORMATION

THE CSA GROUP OF COMPANIES are responsible to ensure that necessary records and documents of their data subjects are adequately protected and maintained to ensure that records that are no longer needed or are of no value are disposed of at the proper time. These rules apply to all documents which are collected, processed or stored by THE CSA GROUP OF COMPANIES and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

THE CSA GROUP OF COMPANIES does not automatically discard or dispose of the telephone numbers and email addresses of data subjects with whom it has previously dealt as these are stored on cellphones and the system of THE CSA GROUP OF COMPANIES but will do so on request by the data subject. Data subjects are entitled to request removal of their personal information.

Rules governing the secure disposal of personal information and in particular the devices on which these are stored are necessary in order to maintain data security and support compliance with this THE CSA GROUP OF COMPANIES Policy. THE CSA GROUP OF COMPANIES acknowledges that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely. Data subjects, who interact with THE CSA GROUP OF COMPANIES acknowledge the following disposal rules:

8.1. Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.
8.2. THE CSA GROUP OF COMPANIES undertake to ensure that all electrical waste, electronic equipment and data on disk drives be physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.
8.3. THE CSA GROUP OF COMPANIES will ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.
8.4. In the event that a third party is used for data destruction purposes, the Information Officer will ensure that such third party will also comply with this policy and any other applicable legislation.
8.5. THE CSA GROUP OF COMPANIES may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. THE CSA GROUP OF COMPANIES undertake to notify employees of applicable documents where the destruction has been suspended to which they have access to.

8.6. In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed.
8.7. The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

9. INTERNET AND CYBER TECHNOLOGY

These clauses constitute a summary of the Internal THE CSA GROUP OF COMPANIES Internet/IT/Cyber Security Policy applicable to all internal employees and clerks.

9.1. Acceptable use of THE CSA S GROUP OF COMPANIES' Internet Facilities & standard Anti-Virus rules

The repercussions of misuse of THE CSA GROUP OF COMPANIES' systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), financial penalties for data leakage and lost productivity resulting from network downtime.

In order to ensure that THE CSA GROUP OF COMPANIES' IT systems are not misused, everyone who uses or has access to THE CSA GROUP OF COMPANIES' systems have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

9.1.1. Information will be protected against any unauthorized access as far as possible;
9.1.2. Confidentiality of information will be assured as far as possible;
9.1.3. Integrity of information will be preserved as far as possible;
9.1.4. Availability of information for business processes will be maintained;
9.1.5. Compliance with applicable laws and regulations to which THE CSA GROUP OF COMPANIES is subject will be ensured by the Information Officer as far as possible.

Every user of THE CSA GROUP OF COMPANIES's IT systems takes responsible for exercising good judgment regarding reasonable personal use.

9.2. IT Access Control

Management of THE CSA GROUP OF COMPANIES undertakes to ensure that logging into the IT system and software packages is password controlled and shall exercise all caution in allowing unauthorized access to the password.

9.3. THE CSA GROUP OF COMPANIES' Email Rules

THE CSA GROUP OF COMPANIES acknowledge that most of its communications are conducted via email and instant messaging (IM). Given that email and IM may contain extremely sensitive and confidential information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware, so THE CSA GROUP OF COMPANIES must be protected as completely as possible from these threats. The misuse of email and IM can pose many legal, privacy and security risks, so it is important for users to be aware of the appropriate use of electronic communications.

It is of use to note that all users of THE CSA GROUP OF COMPANIES' email system are prohibited from using email to:

9.3.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
9.3.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
9.3.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
9.3.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
9.3.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
9.3.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass THE CSA GROUP OF COMPANIES negatively impact productivity, or harm morale.

The purpose of these rules is to ensure that information sent or received via THE CSA GROUP OF COMPANIES' IT systems is appropriately protected, that these systems do not introduce undue security risks to THE CSA GROUP OF COMPANIES and that users are made aware of what group deems as acceptable and unacceptable use of its email and IM.

9.4. THE CSA GROUP OF COMPANIES' Rules related to handheld devices

Many users do not recognize that mobile devices represent a threat to IT and data security. As a result, they often do not apply the same level of security and data protection as they would on other devices such as desktop or laptop computers. The

rules hereunder outline THE CSA GROUP OF COMPANIES' requirements for safeguarding the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices that PC's and Notebooks.

9.4.1. THE CSA GROUP OF COMPANIES' users of handheld devices are expected to diligently protect their devices from loss and disclosure of private information belonging to or maintained by THE CSA GROUP OF COMPANIES.

9.4.2. In the event of a security incident or if suspicion exists that the security of THE CSA GROUP OF COMPANIES' systems has been breached, the particular employee affected shall be obliged to notify the IT support and Information Officer immediately especially when a mobile device may have been lost or stolen.

9.5. **Anti-virus rules**

9.5.1. Management of THE CSA GROUP OF COMPANIES is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into THE CSA GROUP OF COMPANIES' programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

9.5.2. It is worth noting that users are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from THE CSA GROUP OF COMPANIES' networks, stop using the infected computer immediately and notify the IT support.

9.5.3. It is further worth noting that THE CSA GROUP OF COMPANIES' users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments. If a virus is suspected the attachment must not be opened or forwarded and must be deleted immediately.

9.6. **Physical access control**

All of THE CSA GROUP OF COMPANIES' premises that include computers and other types of information technology resources will be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats.

9.7. **Usage Data**

Usage Data is collected automatically when using the internet services of THE CSA GROUP OF COMPANIES. Usage Data may include information such as data subjects' device's internet protocol address (e.g. IP address), browser type, browser version, details of the pages of THE CSA GROUP OF COMPANIES' website that are visited by data subjects, the time and date of the website visit, the time spent on those pages, unique device identifiers and other diagnostic data. When data subjects access the website services of THE CSA GROUP OF COMPANIES by or through a mobile device, THE CSA GROUP OF COMPANIES may collect certain information automatically, including, but not limited to, the type of mobile device used by the data subject, unique ID, the IP address of the mobile device, the mobile operating system, the type of mobile Internet browser used, unique device identifiers and other diagnostic data. THE CSA GROUP OF COMPANIES may also collect information that the user's browser sends whenever THE CSA GROUP OF COMPANIES' website is visited.

9.8. **Tracking Technologies and Cookies**

Cookies and similar tracking technologies are used to track the activity on THE CSA GROUP OF COMPANIES' website and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyze the efficiency of the website. The technologies which may be used to track may include:

9.8.1. Cookies or Browser Cookies. A cookie is a small file which may be placed on a data subject's device. Data subjects can instruct their browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if this function of THE CSA GROUP OF COMPANIES' website is not accepted, data subjects may not be able to use some parts of the website. Unless the browser settings have been adjusted, THE CSA GROUP OF COMPANIES' website may use Cookies.

9.8.2. Flash Cookies. Certain features of the website may use local stored objects (or Flash Cookies) to collect and store information about data subjects' preferences or activity on the website. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies. For more information on how Flash Cookies can be deleted the following process can be followed: "Where can I change the settings for disabling, or deleting local shared objects?" available at https://helpx.adobe.com/flashplayer/kb/disable-local-shared-objects;

9.8.3. Web Beacons. Certain sections of the website and emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit THE CSA GROUP OF COMPANIES for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

9.8.4. Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on data subjects' personal computer or mobile device even when offline, while Session Cookies are deleted as soon as data subjects' web browsers are closed.

10. THIRD PARTY OPERATORS

THE CSA GROUP OF COMPANIES recognize that, in fulfilling its contractual services to its clients and in order to operate efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to THE CSA GROUP OF COMPANIES's service delivery. As referenced in clauses 5 and 6 above, THE CSA GROUP OF COMPANIES will obtain the necessary Consent where required from the particular data subject when information collected is shared with third parties.

THE CSA GROUP OF COMPANIES shall moreover and where possible enter into an OPERATORS' AGREEMENT with the relevant third party with which group shares data subjects' information for purposes of processing such information in order to ensure that the third party operator treats the personal information of THE CSA GROUP OF COMPANIES' data subjects responsibly and in accordance with the provisions contained in the Act and Regulations thereto. THE CSA GROUP OF COMPANIES shall, where possible request copies of the third party operators' POPIA Policy, rules, internet rules and details of the third party's Information Officer.

11. BANKING DETAILS

It is a known fact that emails and other types of electronic communication are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of the transaction. THE CSA GROUP OF COMPANIES has implemented clear notifications within all its correspondences (emails and physical letters) warning data subjects of the risks of email hacking and interceptions.

12. DIRECT MARKETING

THE CSA GROUP OF COMPANIES is committed to not sharing data subjects' information with third parties for the sole purpose of such third party marketing to data subjects. In the event that any associated third party using the data subjects' information shared by THE CSA GROUP OF COMPANIES with such third party in the fulfilment of its services, THE CSA GROUP OF COMPANIES takes no responsibility for any consequences suffered by the data subject which may have been caused by the third party's actions.

THE CSA GROUP OF COMPANIES sends out direct marketing emails, smses or whatsapps to data subjects on its system from time to time and has implement the required OPT IN our OPT OUT options which must at all times be clearly available to the recipient data subjects. Appropriate measures have been taken in respect of social media pages on which posts are placed and necessary POPIA notices have been placed for the benefit of any social media follower.

13. DATA CLASSIFICATION

All of group's employees share in the responsibility for ensuring that THE CSA GROUP OF COMPANIES' information assets receive an appropriate level of protection as set out hereunder:

13.1. Managers of THE CSA GROUP OF COMPANIES shall be responsible for assigning classifications to information assets according to the standard information classification system presented below.
13.2. Where practicable, the information category shall be embedded in the information itself.
13.3. All employees of THE CSA S GROUP OF COMPANIES shall be guided by the information category in their security-related handling of THE CSA GROUP OF COMPANIES's information. All information of THE CSA GROUP OF COMPANIES and all information entrusted to THE CSA GROUP OF COMPANIES from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

Information Description	Examples	Category
Unclassified Public	Information is not confidential and can be made public without any implications for THE CSA GROUP OF COMPANIES	Product brochures widely distributed Information widely available in the public domain, including publicly available web site areas of THE CSA GROUP OF COMPANIES Sample downloads of THE CSA GROUP OF COMPANIES' software that is for Sale Financial reports required by regulatory authorities Newsletters for external transmission
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence THE CSA GROUP OF COMPANIES' operational effectiveness, cause an	Passwords and information on corporate security procedures Know-how used to process client information Standard Operating Procedures used in all parts of THE CSA GROUP OF COMPANIES' activities

	important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	All software codes developed by THE CSA GROUP OF COMPANIES , whether used internally or sold to clients
Client Confidential Data	Information collected and used by THE CSA GROUP OF COMPANIES in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. Access to this information is very restricted within THE CSA GROUP OF COMPANIES. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data Accounting data and internal financial reports Confidential customer business data and confidential contracts Non-disclosure agreements with clients\vendors Company business plans Children's information

14. <u>RIGHTS OF THE DATA SUBJECT- FORMS 1 & 2 ATTACHED</u>

14.1. The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information is not affected.

14.2. A data subject may object, at any time, to the processing of personal information–

- In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
- For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

14.3. A data subject, having provided adequate proof of identity, has the right to –

- Request THE CSA GROUP OF COMPANIES to confirm, free of charge, whether or not it holds personal information about the data subject; and
- Request from THE CSA GROUP OF COMPANIES a record or a description of the personal information about the data subject held by it, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information – within a reasonable time, at a prescribed fee as determined by the Information Officer, in a reasonable manner and format and in a form that is generally understandable.

14.4. A data subject may, in the prescribed manner, request THE CSA GROUP OF COMPANIES to –

- correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
- destroy or delete a record of personal information about the data subject that THE CSA GROUP OF COMPANIES is no longer authorised to retain.

14.5. Upon receipt of a request referred to in clause 14.4, THE CSA GROUP OF COMPANIES will, as soon as reasonably practicable –

- correct the information;
- destroy or delete the information;
- provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or
- where an agreement cannot be reached between THE CSA GROUP OF COMPANIES and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

14.6. THE CSA GROUP OF COMPANIES will inform the data subject, who made a request as set out in clause 14.5, of the action taken as a result of the request.

15. <u>COVID 19</u>

THE CSA GROUP OF COMPANIES have implemented and continue to apply its Workplace Risk Assessment measures in line with accepted Occupational Health and Safety Guidelines issued by the Departments of Labour and Health and in terms of the Regulations and Guidelines to the Disaster Management Act. With reference to these assessment measures, THE CSA OF COMPANIES is entitled to oblige employees, clients and visitors to any of its sites to complete a Covid 19 Risk Assessment form provided that the personal, medical and special personal information required to be completed are necessary and limited to the purposes of assessing the risk of Covid 19 exposure. THE CSA GROUP OF COMPANIES may also, where required by statute, share the information with the Departments of Labour and Health especially in the event of someone testing positive and/or where a significant increase of risk exists in the workplace and offices.

With the implementation of THE CSA GROUP OF COMPANIES Workplace Vaccination program, further employee and other relevant data subjects' personal and medical information may be collected and processed by THE CSA GROUP OF COMPANIES

and may be shared with Regulated third parties and internally if the sharing of the information complies with the provisions for THE CSA GROUP OF COMPANIES' Vaccination program Policies.

16. INFORMATION OFFICER

16.1. **Appointed Information Officer:**

INFORMATION OFFICER: Name available upon written request
Contact details: 021 433 0347
Postal Address: PO BOX 756, SEA POINT, CAPE TOWN, RSA, 8060

16.2. **The general responsibilities of THE CSA GROUP OF COMPANIES' Information Officer delegated include the following:**

16.2.1. The encouragement of compliance, by THE CSA S GROUP OF COMPANIES, with the conditions for the lawful processing of personal information;
16.2.2. Managing requests made to THE CSA GROUP OF COMPANIES pursuant to POPIA;
16.2.3. Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the business.
16.2.4. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
16.2.5. Review policy rules regularly, document the results, and update the policy as needed.
16.2.6. Continuously update information security policies and network diagrams.
16.2.7. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
16.2.8. Perform continuous computer vulnerability assessments and audits.
16.2.9. The Information Officer may appoint any number of Deputy Information Officers as is necessary to perform the duties of the Information Officer as set out above. The Information Officer has control over every Deputy Information Officer(s) appointed.
16.2.10. The Information Officer may delegate, in writing, his/her power of duty conferred or imposed by this Act, to a Deputy Information Officer(s). In his/her decision to delegate power of duty, the Information Officer must give due consideration to the need to render THE CSA GROUP OF COMPANIES as accessible as reasonably possible for requests of its records.
16.2.11. The Deputy Information Officer's duties must only be exercised or performed subject to any conditions set by the Information Officer. The delegation of power does not prohibit the Information Officer from performing these duties himself/herself. The Information Officer may at any time withdraw or amend, in writing, the delegation of power of duty.
16.2.12. Any right or privilege acquired, or any obligation or liability incurred as a result of the delegation of power, is not affected by any subsequent withdrawal or amendment of that delegation.

16.3. **The data breach responsibilities of THE CSA GROUP OF COMPANIES' Information Officer include the following:**

16.3.1. Ascertain whether personal data was breached;

16.3.2. Assess the scope and impact by referring to the following:
- 16.3.2.1. Estimated number of data subjects whose personal data was possibly breached
- 16.3.2.2. Determine the possible types of personal data that were breached
- 16.3.2.3. List security measures that were already in place to prevent the breach from happening.

16.3.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:
- 16.3.3.1. The Information Regulator;
- 16.3.3.2. Any data subjects who have been affected by such data breach;
- 16.3.3.3. THE CSA GROUP OF COMPANIES will only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.
- 16.3.3.4. The notification to a data subject will be in writing and communicated to the data subject in at least one of the following ways: a) Posted to the data subject's last known physical or postal address; or b) Sent by e-mail to the data subject's last known e-mail address; or c) Placed in a prominent position on the website of THE CSA GROUP OF COMPANIES; or d) Published in the news media.
- 16.3.3.5. Communication should include the following:

- Contact details of Information Officer
- Details of the breach,
- Likely impact,
- Actions already in place, and those being initiated to minimise the impact of the data breach.
- Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.
- A description of the possible consequences of the security compromise;
- A description of the measures that THE CSA GROUP OF COMPANIES intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- If known to THE CSA GROUP OF COMPANIES, the identity of the unauthorised person who may have accessed or acquired the personal information.

16.3.4. Review and monitor

16.3.4.1. Once the personal data breach has been contained, THE CSA GROUP OF COMPANIES will conduct a review of existing measures in place, and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.

16.3.4.2. All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

17. GDPR

THE CSA GROUP OF COMPANIES fully supports and complies with the 6 (Six) protection principles of the GDPR related to data subjects of THE CSA GROUP OF COMPANIES who fall within the EU and which are summarised below:

17.1. **Lawfulness, fairness and transparency**: The personal information of the European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

17.2. **Purpose limitation:** The personal information of the European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.

17.3. **Data Minimisation**: The personal information of the European citizens will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

17.4. **Accuracy**: The personal information of the European citizens will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.

17.5. **Storage Limitation**: The personal information of the European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

17.6. **Integrity and Confidentiality**: The personal information of the European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

18. AVAILABILITY AND REVISION

A link to this Policy is made available on THE CSA GROUP OF COMPANIES company website www.csa.global

This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.