Company Name: Calypso Creative Agency cc
Company Reg Nr: 2009/194454/23
Date: 23 June 2021

1. Policy: Information Incident Management Process

1.1. PURPOSE

This Policy was developed to provide direction to guide all employees, contractors, visitors, Data Operators, and other persons authorised to access and use the systems of the Company, on how to respond to incidents that threaten the security of Personal Information.

The purpose of this Policy is to:

- Provide a framework for responding to Information Incidents (including data breaches) in accordance with POPIA.
- Assist the Users in understanding their responsibilities in addressing and dealing with Information Incidents.

This Policy applies to all Users, and any person handling information or data processed by the Company.

This Policy should be read in conjunction with other policies of the Company that regulate the protection of Personal Information.

1.2. POLICY

The incident management of an Information Incident is vital to the Company. By handling such incidents correctly, the impact on the reputation of the Company, and other damage to the Company can be managed. Implementing the necessary control measures in the case of an information or data breach is critical.

1.3. INFORMATION INCIDENTS

This section of the Policy sets out the steps that must be taken in response to an Information Incident in relation to the Company, including the roles and responsibilities of all stakeholders involved.

An Information Incident means a single or a series of unwanted or unexpected events that threaten information security or privacy. Information Incidents include any collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorised by the Company.

Information Incidents include Privacy Breaches, which are unauthorised collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alteration, consultation, use or dissemination by means of transmission, merging, linking, disposal (erasure or destruction), or storage of Personal Information, whether accidental or deliberate. If these breaches include Personal Information, POPIA will be applicable to both Information Incidents and Privacy Breaches.

1.4. INFORMATION OFFICER

The Information Officer of the Company is responsible for the coordination, investigation, and resolution of all Information Incidents.

The Information Officer will be responsible for determining when a decision must be made to either notify or not notify Data Subjects of an Information Incident based on a balance of harms or as required by relevant legislation, including POPIA (*Refer to Annexure B and Annexure C*).

The Information Officer is solely responsible for liaising with the Information Regulator regarding an actual or suspected Privacy Breach or Information Incident.

1.5. PROCESS: INFORMATION INCIDENT REPORTING

Any User or other person who discovers a suspected or actual Information Incident, including a Privacy Breach, must immediately report it to their supervisor and or manager. The supervisor or manager must then report it to the Information Officer immediately (*Refer to Annexure A*). The Information Incident must then be recorded in an Incident Register (*Refer to Annexure D and Annexure E*).

In circumstances where the supervisor or management contact is not immediately available, whether in person or by phone, the User must immediately report the Information Incident directly to the Information Officer.

Where the Information Incident will have serious impact on the Company, the Information Officer must request the User reporting the Information Incident to:

- Assess and document the Information Incident including, the nature, sensitivity, volume, impact, and type of Incident in question (*Refer to Annexure D, E and F*).
- Assist with resolving the Information Incident or containing the Information Incident.
- Provide the User reporting the Information Incident with instructions regarding how to deal with the Information Incident response, such as:
    - Containing the loss.
    - Preventing a recurrence.
    - Determining the next steps.

The Information Officer must decide if additional information should be gathered to determine the response strategy to the Information Incident, including the (*Refer to Annexure D, E and F*):

- Type of Information Incident.
- Nature and sensitivity of the Information Incident.
- Volume.
- Impact and implications of unauthorised disclosures or asset losses.

The Information Officer determines whether the Information Incident is major or minor, based on the following:

- The Information Incident involves Personal Information, sensitive, confidential, proprietary, or critical information of the Company.
- If there is a reasonable expectation of harm to any data subject because of the Information Incident.
- Whether data subjects will be, notified that their Personal Information has been compromised.
- Whether the incident will be reported to the Information Regulator.
- Whether the Information Incident has a serious or potentially serious public impact.

Minor Information Incidents:

- The User in question will be the main point of contact for the breach in question.
- The User will refer all minor Information Incidents to the Information Officer for follow-up and resolution in collaboration with CEO of the Company.
- The Information Officer must request the User to provide a report regarding the Information Incident.

Major Information Incidents:

- The Information Officer must coordinate an Incident Management and Investigation Process to conduct an assessment and gather evidence regarding the Information Incident.

1.6. NOTIFICATION OF THE REGULATOR

The Information Officer will determine if there was a breach of any Data Subject's Personal Information, and whether such breach should be reported to the Regulator (*Refer to Annexure D, E and F*). The following factors need to be considered before reporting any Information Incident to the Regulator:

- The nature of the Information Incident in question.
- The legitimate needs of law enforcement to act on the Information Incident.
- Measures that are reasonably necessary to determine the scope and extent of the compromise.
- Measures that should be taken to restore the integrity of the Company's information systems.

The Information Officer must ensure that any breach or compromise is reported to the Regulator as soon as reasonably possible after the discovery of the compromise (*Section 22 of POPIA*), if determined, as necessary.

1.7. NOTIFICATION OF DATA SUBJECTS

The impact of Privacy Breaches must be reviewed to determine if it is appropriate to notify individual Data Subjects whose Personal Information has been affected. The User will work with the Information Officer to notify affected parties and take other required action that may be appropriate in the circumstances (*Refer to Annexure B and C*).

The key consideration in deciding whether to notify an affected individual is whether such notification is necessary to avoid harm to an individual, such as:

- Identity theft or fraud.
- Physical harm.
- Damage to reputation.
- Business or employment opportunities.

Other considerations in determining whether to notify individual data subjects include the following:

- Any legislative requirements for notification such as required by Section 22 of POPIA.
- Any contractual obligations that may require notification.
- A risk of loss of confidence in the Company.
- Good customer relations dictate that notification is appropriate.

Notification is determined by the *balance of harms*. Under this principle, an individual Data Subject who could potentially face harm because of an Information Incident may not be notified if it is determined that the harm that would result from a notification would outweigh the benefit to be gained from the notification.

If it is determined that notification of individual Data Subjects would be appropriate in the circumstances of an Information Incident, the:

- Notification should occur as soon as possible following the breach.
- All affected individuals should be notified directly.

1.9. CLOSURE OF INFORMATION INCIDENT FILE

When closing an Information Incident file, the Information Officer must notify the CEO. The Information Officer will also write a final report (*Refer to Annexure F*), including recommendations, and submit it to all stakeholders. There are 2 types of recommendations included in the Report, namely:

- Essential recommendations, which must be implemented promptly.
- Advisory recommendations, which the CEO will decide whether to implement.

1.10. COMPLIANCE

The Information Officer will be responsible for implementing the recommendations set out in the Report. The Information Officer may perform compliance reviews or may audit the implementation of the recommendations set out in the Report and their effectiveness once implemented.

1.11. RESPONSIBILITIES

User

In the case of any actual or suspected Information Incident, the User's responsibilities are to:

- Report the Information Incident immediately to the Information Officer or their manager.
- Recover the Personal Information or Confidential Information, if possible,
- Contain the Information Incident to lessen its impact and implication for the Company and the Data Subjects involved.
- Remediate the Information Incident by working with the Information Officer to determine the specifics of the Information Incident to resolve it.
- Prevent Information Incidents by being diligent in the handling of Personal Information, and Confidential Information.
- Be an active participant in developing the culture of prudent information management.

Contractor or Service Provider (Data Operator):

Where the User in question is a Data Operator, in the case of an Information Incident, the Data Operator's responsibilities are to:

- Ensure that their employees, service providers, or any other persons who discover an Information Incident (including a Privacy Breach) immediately notify the management of such Data Operator, who must then report it to the Information Officer of the Company.
- Ensure that the Information Incident is immediately recorded in the Register (*Refer to Annexure D and E)*.
- Recover the Personal Information or Confidential Information, if possible.
- Contain the incident to lessen the impact for the Company and any Data Subjects.
- Remediate the Information Incident.
- Work collaboratively with the Information Officer.
- Support the investigation and Information Officer.
- Notify any Data Subjects (whether individuals or juristic persons) affected by the Information Incident, as directed by the Information Officer.
- Prevent Information Incidents by:
    - Ensuring that employees know and understand how to apply changes in the handling of Personal Information, and Confidential Information.
    - Being diligent in the handling of Personal Information and Confidential Information.
    - Implementing recommendations from the Information Incident reporting process and the Information Officer.
    - Developing a culture for the prudent management of information within the Data Operator's business.
    - Providing training.
    - Ensuring that their employees understand their responsibility in reporting Information Incidents, including containing the loss and recovering the information.

The Information Officer:

The Information Officer's responsibilities in respect of any Information Incident are to:

- Receive the report about the Information Incident from the User and provide direction on assessing the Information Incident.
- Ensuring its recorded in the Register (*Refer to Annexure D and E)*.
- Determine if the Personal Information, or Confidential Information in question can be recovered.
- If the loss or disclosure can otherwise be contained.
- The coordination, investigation, and resolution of all Information Incidents, including Privacy Breaches.
- Receive and review status reports and compile the Report and present to the CEO the implementation of the recommendations contained in the Report.
- Ensure that the recommended controls in the Report are implemented.
- Report Information Incidents to the CEO (*Refer to Annexure D and E)*.
- Contact all responsible stakeholders to ensure communication, recommendation, and collaboration.
- Liaise with the Information Regulator on Privacy Breaches and other Information Incidents.

The Information Officer must prevent Information Incidents by:

- Implementing the recommendations set out in the Report.
- Ensuring that Users know and understand how to apply changes in the handling of Personal Information, and Confidential Information.
- Participating in the development of a culture within the Company for the prudent management of information.
- Providing appropriate training.
- Ensuring that Users understand their responsibility in reporting all Information Incidents, including the importance of containing the loss and recovering the information.
- Notifying any Data Subjects (both individuals and juristic entities) affected by the Information Incident.
- Ensuring that Data Operators understand their responsibilities in the Information Incident reporting process and collaborating with them to ensure timely and accurate reporting.

1.12. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

1.14. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

1.15. POLICY AWARENESS AND UPDATE

Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

1.16. INTERNAL DOCUMENT APPROVAL

Information Officer Name	Signature	Date
Mrs Paula Gageiro		23 June 2021

1.17. DOCUMENT VERSION CONTROL

Version	Date	Summary of Changes