MANDALA CONSULTING
INTEGRATION FOR SUSTAINABILITY

Data Breach Management Policy

1) Policy Statement:

- As an organisation which processes personal data, every care is taken to protect personal data and to avoid a data protection breach. This policy outlines the measures we take against unauthorised or unlawful processing or disclosure and against accidental loss, destruction of or damage to personal data.
- In the event of data being lost or shared inappropriately, we will take appropriate action to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by us and our staff, employees, affiliates and contractors, referred to herein after as "**staff'**.
- This Policy forms part of our Data Protection Procedure and Protocol and all staff are made aware of these procedures through induction, supervision and ongoing training.

2) Purpose:

- It is a regulatory requirement under the Protection of Personal Information Act 4 of 2013 ("**POPIA**") for responsible parties to have consistent and effective governance and control arrangements to protect the personal data that it processes. This Policy therefore sets out the course of action to be followed by all staff in the event of a real or potential data protection breach.

3) Personal Data:

- Personal data means any information relating to an identified or identifiable natural person (i.e. human being) or juristic person (i.e. legal entity for e.g. a company). An identifiable natural personal or juristic person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, registration number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- As examples, this might include personnel data such as name, address information, telephone number, date of birth, marital status, bank account, identity number, registration number and social security numbers, medical records and testimonials, for employees, customers or third parties.
- It also might include data about persons who are our suppliers or customers or work for or are customers of our corporate customers or suppliers, such as name, address information, telephone number, order history, payment details, photos and medical data.

4) Definition of Personal Data Breach:

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes and/or any other type of breach of personal information as recognised under POPIA.
- A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In summary, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
- Personal data breaches can include:

    - Loss or theft of personal data and/or equipment on which data is stored
    - Access by an unauthorised third party
    - Deliberate or accidental action (or inaction) by a controller or processor
    - Sending personal data to an incorrect recipient
    - Computing devices containing personal data being lost or stolen
    - Alteration of personal data without permission
    - Loss of availability of personal data
    - Hacking attack

- Cyber attack
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Flawed data destruction procedures.

5) Aim of Data Breach Management Policy:

- The aim of this Policy is to ensure a standardised and consistent approach is followed when responding to data breaches to enable us to:

  - Report data breaches without delay to the Information Officer
  - Identify incidents of data breaches quickly and investigate them properly and in a timely manner
  - Record and document all incidents and report them to the Information Officer and his/her data protection team ("**DPT**") responsible for managing data protection and/or data security and/or data breach incidents within the organisation
  - Assess the severity and impact of the data breach and inform the Information Regulator under POPIA and/or any other required law enforcement agencies, supervisory authorities and, subject to the law, effected data subject(s)
  - Take action which is proportionate, consistent and transparent to prevent further damage
  - Regularly monitor and review all data breach incidents and potential situations that may lead to a data breach to identify improvements in policies, procedures and control mechanisms to remove or mitigate risk of further repetition.

6) Managing a Data Breach:

Step 1: Containment and Recovery:

- The Information Officer will ascertain the severity of the breach, whether any personal data is involved and whether the breach is still occurring.
- If the breach is still occurring, the Information Officer will establish what steps need to be taken immediately to minimise the effect of the breach and contain the breach from further data loss (e.g. alert the Company's IT Technical support, restricting access to systems or close down a system etc).
- The Information Officer, together with the DPT, will consider and implement appropriate steps required to recover any data loss where possible and limit damage caused (e.g. use of back-ups to restore data; changing passwords etc.).
- In line with the provisions of Step 4 below, the Information Officer together with the DPT must consider and implement the data breach notification procedure as required by POPIA.
- The Information Officer and DPT shall, based on the severity and likely impact of the breach, inform the board of the Company. At the same time, depending on the nature and extent of the breach, the Information Officer may seek expert or legal advice and/or a public body responsible for the prevention, detection or investigation of offences if it is believed that illegal activity has occurred or likely to occur.
- Where a significant breach is occurred, the Information Officer will inform the Information Regulator within 72 (seventy two) hours of the discovery of the breach (refer to data breach notification procedure at Step 4 below).
- Any decisions taken and reasons therefore in relation to a data breach must be documented by the Information Officer. In this regard all the key actions and the decisions are required to be fully documented and logged in the Company's data security breach log.

Step 2: Preliminary Assessment of Risk

- Further actions may be needed beyond immediate containment of the data breach. To help the Company determine the next course of action, an assessment of the risks associated with the breach is undertaken to identify whether any potential adverse consequences for persons are likely to occur and the seriousness of these consequences. The information officer will consider the points arising from the following questions:

    - What type and volume of data is involved?
    - How sensitive is the data? Could the data breach lead to distress, financial or even physical harm?
    - What events have led to the data breach? What has happened to the data?
    - Has the data been unofficially disclosed, lost or stolen? Were preventions in place to prevent access/misuse? (e.g. encryption)
    - How many persons are affected by the data breach?
    - Who are the persons whose data has been compromised?
    - What could the data tell a third party about the persons? Could it be misused regardless of what has happened to the data?
    - What actual/potential harm could come to those persons? E.g. physical safety; emotional wellbeing; reputation; finances; identity theft; one or more of these and other private aspects to their life
    - Are there wider consequences to consider?
    - Are there others that might advise on risks/courses of action (such as banks if person's banking details have been affected by the breach)?

Step 3: Data Breach Notification

Company acting as a Responsible party:

- In the event of a personal data breach, if the Company is the responsible party in respect of the personal data in question, it shall without undue delay and, where feasible, not later than 72 (seventy two) hours after having becoming aware of it, notify the Information Regulator under POPIA in accordance with Section 22 of

POPIA and where required to do so, the effected data subject(s) unless the personal data breach notification to the data subject shall, according to a public body responsible for the prevention, detection or investigation of offences or the Information Regulator, determines that same would impede a criminal investigation by the public body concerned. Where the notification to the Information Regulator is not made within 72 (seventy two) hours, it shall be accompanied by reasons for the delay.

- The notification shall at least:

    - Describe the nature of the personal data breach including where possible, the categories and approximate number of Data subjects concerned and the categories and approximate number of personal data records concerned
    - Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained
    - Describe the likely consequences of the personal data breach
    - Describe the measures taken or proposed to be taken by the Company as the Responsible party to address the personal data breach, including, where appropriate, measures to mitigation its possible adverse effects
    - A recommendation with regard to the measures to be taken by the Data subject to mitigate the possible adverse effects of the security compromise
    - If known to the Responsible party, the identity of the unauthorised personal who may have access or acquire the personal data.

- Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without further undue delay.

The Responsible party shall document any personal data breaches, comprising the facts relating to the personal data breach, its affects and the remedial action taken. That documentation shall enable the Information Regulator to verify compliance with the provisions of POPIA.

Company acting as an Operator:

- Where the Company is acting as the operator, it shall notify the responsible party without undue delay after becoming aware of a personal data breach and provide information about the breach only to the Responsible party. The Responsible party is then responsible for notifying the data breach to the Information Regulator. Under no circumstances should the Company, when it is acting as an operator for a Responsible party notify a personal data breach directly to the Information Regulator or a data subject, unless otherwise advised by such Responsible party in writing.
- As soon as any member of staff discovers or receives a report of a data breach, they must inform the Information Officer as soon as possible and without delay. If the breach occurs or is discovered outside normal working hours, then notification should be sent as soon as is practicable.
- An emailed report can be submitted to the Information Officer at stefan@mandalaconsulting.co.za in the first instance and should include accurate details of the incident. The Information Officer can be contacted telephonically at 0769073277.
- An initial assessment of the data breach by the Information Officer will include a written collection and report of as much information as possible about the incident in order to fully assess the impact of the data breach and determine actions required.

Step 4: Evaluation and Response:

- When the Company's response to a data breach has reached a conclusion, the Information Officer together with DPT, will undertake a full review of both the causes of the breach and the effectiveness of the response. The full review is reported to the Company board for information and discussion as soon as possible after the data breach has been identified.

- If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified as a cause of the data breach, then appropriate action plans will be drafted, actioned and monitored to rectify any issues and implement recommendations for improvements. Where the Information Officer deems necessary and as required by the Company's procedure, the board will be party to discussions regarding action plans and be able to monitor progress against the actions appropriately.
- If a breach warrants a disciplinary investigation, legal advice will be sought through Human Resources channels.

7) Implementation of these Procedures:

- The Information Officer will be responsible for ensuring that staff are aware of these procedures for reporting and managing data breaches. Data protection training for all staff is mandatory, including new employees and all staff will undertake refresher training annually.
- If staff have any queries or questions relating to these procedures, they should discuss this with their Department Head/line manager and/or the Information Officer.

8) Complaints about our Data Breach Management Procedure:

- If any person believes that a data breach has not been dealt with properly, a complaint should be made to the Company through our normal complaints procedure. This does not affect any right a person may have in terms of POPIA to lodge a complaint directly with the Information Regulator.

Last updated: July 2021

MANDALA CONSULTING

INTEGRATION FOR SUSTAINABILITY