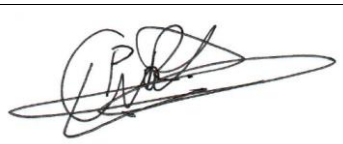
DATA BREACH POLICY

Policy Owner:	Human Resources (HR)		
Effective Date:	1 July 2021		
Version:	Version 1		
Authorised by:	Information Officer		30/06/2021
		Signature	Date
	Deputy Information Officer		30/06/2021
		Signature	Date
Note:	TMS Dynamics reserves the right to amend the contents of this policy as and when required. The policy currently in effect will apply to all employees regardless of the policy that applied at the time of employment.		

1. Scope/objective of the policy

1.1 The purpose of the policy is to provide protection over the information held and the processing of data by TMS Dynamics, as well as contain all data breaches and minimise the risks associated with any breaches.

1.2 This policy also outlines the actions that should be taken in the event of a breach to ensure data is secure and to prevent further breaches.

1.2 The policy is intended to ensure that every care is taken to protect personal data from incidents (accidental or deliberate) to avoid a security breach that could compromise data.

1.3 The Protection of Personal Information (POPI) Act (2003), and Promotion of Access to Information Act (PAIA) (2000), requires organisations to have mandatory data breach notifications in place, this will include the informing of such a breach to the Information Regulator as well as any parties whose personal information have been accessed or acquired by an unauthorised party. This notification should include:

1.3.1 A description of the possible consequences of the security compromise;

1.3.2 A description of the measures taken or proposed to be taken by the responsible party to remedy the security breach;

1.3.3. A recommendation of the measures that any party whose personal information was leaked in the security breach;

1.3.4. The identity of the unauthorised person, if known, who accessed or acquired the personal information.

2. Definitions

2.1 **Data:** information in digital form that can be transmitted or processed.

2.2 **Data subject:** a person to whom personal information relates/ a juristic person ie. a company.

2.3 **Personal Data**: any information relating to an individual by which the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access.

2.4 **Data Breach:** Any incident, event, or action, whether accidental or deliberate that has the potential to compromise the availability of data, the integrity of data, confidentiality, and/or our company's data systems.

2.5 **Information Regulator:** The South African independent body established in terms of section 39 of the Protection of Personal Information Act ,4 of 2013 who is empowered to monitor and enforce compliance with POPI and PAIA Acts.

2.6 **Information Officer:** of, or in relation to a:

a) public body is the head of that public body. This means for a national or provincial government department, the Information Officer is the Director-General of the department or the equivalent official, and for a municipality, the manager is the Information Officer. In any other public body, the Chief Executive Officer (CEO) is the Information Officer.

b) private body means that by default the owner of the business. Therefore, based on the type of private body, the Information Officer will be the sole trader, a partner in a partnership or the CEO (or equivalent) in a company or close corporation.

2.7 **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.

3. Legal principles

The following legislation is applicable to this policy:

3.1 The Protection of Personal Information (POPI) Act (2003)

3.2 Promotion of Access to Information Act (PAIA) (2000)

3.3 Consumer Protection Act (2008)

3.4 Electronic Communications and Transactions Act, 2002 (ECTA)

4 Policy

4.1 This data breach policy applies to everyone at TMS Dynamics – including employees, temporary or casual staff, consultants, suppliers, contractors, freelance workers, or other data processors who are storing or processing data on the behalf of TMS Dynamics .

4.2 For the purposes of this data breach policy, an incident may include (but is not limited to) any of the following:

- Unauthorised use or accessing/modification of data
- Loss or theft of personal or sensitive data
- Loss or theft of equipment on which data has been stored
- Individual error
- Any attempts to gain access to data or our company IT systems (both successful and failed)
- Defacement of web property
- Physical incidents, like a fire, which could compromise IT systems

4.3 All employees who access, manage, or use data in any way are responsible for reporting a data breach or any other type of security incident.

4.4 POPIA clearly states an exception to breach notifications if the identity of data subjects cannot be established.

4.5 According to Section 22 of POPIA, which deals with notification of security compromises, TMS Dynamics must immediately notify stakeholders about unauthorized accesses or acquisitions of personal data.

4.6 Any person who provides false information, or tries to hinder, obstruct, or unlawfully influence the Information Regulator on any matter, will be held liable to a fine or imprisonment.

4.7 Should TMS Dynamics detect a security breach on any of its systems that contain personal information, TMS Dynamics shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

4.8 TMS Dynamics shall notify the affected parties should it have reason to believe that their information has been compromised. Such notification shall only be made where TMS Dynamics can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

4.9 Notification will be provided in writing by means of either:

- Email
- registered mail
- placed on website

4.10 The notification shall provide the following information where possible:

- description of possible consequences of the breach
- measures taken to address the breach
- recommendations to be taken by the data subject to mitigate adverse effects
- the identity of the party responsible for the breach

4.11 In addition to the above, TMS Dynamics shall notify the Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.

5 Procedure

On discovery of a data breach the following actions should be taken:

5.1 *Containment and recovery*

a) In the event of a data breach steps to ensure containment should immediately be actioned by limiting further access to the affected personal information, or the possible compromise of other information.

b) The individual committing the breach or having identified a possible breach should immediately inform their manager or the Information Officer.

c) In order to determine the appropriate response, the following questions should be considered:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

5.2 ***Assessing the risk***

a) An assessment of the data breach will help TMS Dynamics to understand the risks posed by the data breach and how these risks can be addressed, this should be done as soon as practically possible.

b) The assessment is used to establish the severity of the incident. The initial assessment should also include analysing whether there is any way to recover the lost data, and mitigate further risks associated with the incident.

c) The Information Officer or a nominated person will investigate the breach and prepare a Breach Report within 72 hours.

d) The assessment of the data breach will guide the decision on whether to notify affected individuals. In the assessment of a data breach, it is important to consider:

- the type or types of personal information involved in the data breach,
- the circumstances of the data breach, including its cause and extent,
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

5.3. ***Notification of breach to the Information Commissioner's Office (ICO)***

a) Under POPIA, where there are reasonable grounds to believe that a data subject's personal information has been accessed or acquired by an unauthorised person, the responsible party, or any third-party processing personal information under the authority of the responsible party, must notify

the Information Regulator and the data subject thereof, unless the identity of the data subject cannot be established.

b) Notification to the data subject must be:

- made as soon as reasonably possible after the discovery of the breach;
- sufficiently detailed; and
- in writing and communicated to the data subject by mail (to the data subject's last known physical or postal address), email to the data subject's last known email address, placement in a prominent position on the website of the responsible party, publication in the news media, or as may be directed by the Information Regulator.

c) The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:
   - Mailed to the data subject's last known physical or postal address;
   - sent by e-mail to the data subject's last known e-mail address;
   - placed in a prominent position on the website of the responsible party;
   - published in the news media; or as may be directed by the Regulator.

d) The notification should provide the data subject with sufficient detail in order to allow the data subject to take the appropriate protective measures.

e) A responsible party may be directed by the Information Regulator to publicise the breach where the Information Regulator has reasonable grounds to believe that such publicity would protect the data subject.

f) Depending on the exact case, the notification would have to be either physically or electronically mailed to the data subject, published on the organisation's website, or announced to the media.

5.4 Evaluation and response.

a) Once the breach has been dealt with, the cause of the breach needs to be considered. There may be a need to update policies and procedures, or to conduct additional training.

b) It is also important to conduct an extensive review detailing:
   - The cause of the breach
   - The effectiveness of any response

- Whether any changes to existing IT systems, company procedures or policies must be implemented.