INSERT NAME OF ORGANISATION OR PLACE ON ORGANISATION LETTERHEAD

DATA BREACH POLICY

1. INTRODUCTION

1.1 Purpose

1.1.1 [redacted].

1.1.2 The Organisation holds Personal Information in electronic and physical formats. While the Organisation has implemented reasonable technical and organisational measures, there is an inherent risk of unauthorised disclosure and loss of information.

1.1.3 As such, the purpose of this Policy is to:

[redacted]

[redacted]

1.2 Scope

1.2.1 This Policy applies to all employees of the Organisation.

[redacted]

[redacted]

2. DEFINITIONS

In this Policy:

[redacted]

1.4 "**Data Subject**" – means a natural or juristic person to whom Personal Information relates;

1.5 "**Organisation**" – means XXX (registration number XXX);

[redacted]; (d) the biometric information of the person; (e) the personal opinions, views 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;

1.7 "**Policy**" – means this data breach policy, as amended or replaced from time to time;

1.8 "**Processing**" - means any operation or activity concerning Personal Information; and

[redacted]

[redacted].

3. POLICY

3.1. A copy of this Policy will be made available to all employees and all employees are expected to familiarise themselves with the contents of this Policy.

[redacted]

3.3. This Policy forms part of the employee's employment contract with the Organisation.

4. DATA BREACH PROCEDURE

4.1. If an employee has reasonable grounds to believe or suspect that there has been a Data Breach, that employee must immediately complete the Data Breach form contained in Annexure A and deliver said form to the Information Officer of the Organisation.

[redacted]

4.3. Employees must not attempt to contact any Data Subjects or the Information Regulator in the event of a Data Breach. This is the responsibility of the Information Officer. The employee's sole responsibility is to report the Data Breach to the Information Officer, and then only to take such steps as required by the Information Officer, if any.

4.4. On receiving a Data Breach form, the Information Officer shall investigate the suspected Data Breach to establish whether a Data Breach has in fact occurred. On establishing that a Data Breach has in fact occurred, the Information Officer, together with the senior management of the Organisation, shall:

[redacted]

[redacted]

4.4.3. Enter the Data Breach into a register of breaches, kept by the Organisation; and

4.4.4. Notify the relevant persons as per paragraph 5 below.

5. NOTIFICATION OF BREACHES

[redacted]

[redacted]

5.2. Data Subjects

The Information Officer shall notify the relevant Data Subjects in writing of any Data Breaches relating to their Personal Information as soon as reasonably possible after the Data Breach is discovered, provided that such notification may be delayed if a public body or the Information Regulator is investigating the Data Breach.

6. CONSEQUENCES OF BREACHING THIS POLICY

Should any employee breach this Policy, the Organisation shall take the necessary disciplinary action against that employee, and where should the employee be found in breach, he / she may be dismissed. [redacted].

It is the employee's responsibility to contact management should he/she have any queries.

I, _____, (**insert passport number / ID number**) hereby agree that I have read and understood the contents of this Policy and agree to comply with the provisions of this Policy.

Employee signature as receipt hereof	
Date	

Annexure A

Data Breach Form

Employee information:	**Name:** **Position:** **Date:**
Description of suspected Data Breach	
Type of Personal Information concerned	
Details of Data Subjects concerned	
Actions taken	[Do not contact the Data Subject yourself]
Risks identified	

Signed on:

_____

(Insert name of employee)