SCHEDULE C: PRINCIPLES RELATING TO DATA BREACH RESPONSE

Version 1

Effective Date : 01 August 2022

This document contains 8 Pages

Approved by the Board of Trustees on 28 July 2022

SIGNED BY THE CEO:

Signed by:Lindiwe Kwele
Signed at:2022-07-29 09:17:03 +02:00
Reason:Witnessing Lindiwe Kwele

_____ _____ Date: 29/07/22

POLICY REVISION LOG

File Name	Privacy Policy Schedule C- Principles relating to data breach response
Author (s)	Thandi Kuzwayo
Business Unit/ Policy Owner	Legal and Compliance
Effective Date of Policy	01 August 2022
Next Revision Date	01 August 2023

Version	***Date***	***Authors***	***Revision Notes***
1	July 2022	T Kuzwayo	Policy development

1. DEFINITIONS AND ACRONYMS

Unless the context indicates a contrary intention, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings-

1.1. "**ARC**" means the Audit and Risk Committee of the Board;

1.2. **"Board"** means the Board of trustees of the GPF;

1.3. "**Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information under the control of or in the possession of the GPF;

1.4. "**Data Subject**" means a person (natural or juristic) to whom personal information relates;

1.5. "**Employee** " means any permanent or temporary Employee , officer, agent, or independent contractor , who works for the GPF or on a temporary or permanent basis and who receives, or is entitled to receive, any remuneration; and any other person who in any manner assists in carrying on or conducting the business of the GPF and the term 'employed' and 'employment' will have a corresponding meaning;

1.6. "**Exco**" means the Executive Committee of the GPF;

1.7. **"European Union Supervisory Authority"** means the independent public authority within each European Union country that is responsible for monitoring compliance by private bodies and public bodies with the provisions of, and enforcement of the GDPR;

1.8. **"GDRP"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

1.9. **"GPF"** means the Gauteng Partnership Fund;

1.10. **"Information Officer / Data Protection Officer"** means the person appointed by the GPF as such, whose responsibility is to ensure the organisation's compliance with POPIA and the GDPR. Where no information officer has been

appointed, the Chief Executive Officer of the GPF will be responsible for performing the information officer's duties;

1.11. **"Information Regulator"** means the regulatory body established to govern and ensure compliance under POPIA;

1.12. **"Personal Information"** means "personal information" as defined in POPIA and where relevant, GDPR;

1.13. **"Personnel"** means the Employees and Board members of the GPF;

1.14. **"Policy"** means the Principles Relating to Data Breach Response as contained in this document and amended from time to time;

1.15. **"POPIA or "Act"** means the Protection of Personal Information Act No. 4 of 2013 and its Regulations, as amended from time to time;

1.16. **"Response Team"** means the team responsible for investigating Data Breaches as described in this Policy; and

1.17. **"Special Personal Information"** means the special personal information contemplated in section 26 of POPIA and where relevant, the GDPR.

2. OBJECTIVE

The purpose of this Policy is to ensure that any Data Breaches which are experienced by the GPF are identified quickly and addressed in a timely, systematic, and orderly manner in order to effectively manage any risk to both the GPF and the affected Data Subjects, thus promoting transparency and compliance with applicable legislation.

3. SCOPE OF APPLICATION

3.1. This Policy is applicable to all Personnel, contractors, consultants, advisors, and service providers of the GPF that may deal with its Personal Information and records and covers all Personal Information in whatever medium such information is contained.

3.2. This Policy should be read in conjunction with all other relevant policies of the GPF regulating privacy and protection of information.

4. LEGISLATIVE FRAMEWORK

4.1. Constitution of the Republic of South Africa, 1996;

4.2. General Data Protection Regulations;

4.3. Protection of Personal Information Act, 2013;

4.4. Public Finance Management Act no 1 of 1999 (PFMA)

4.5. Other Policy Links

4.5.1. Privacy Policy;

4.5.2. Records Management Policy;

4.5.3. Schedule A: Principles Relating to Records Retention and Disposal;

4.5.4. Schedule B: Principles Relating to Direct Marketing; and

4.5.5. Schedule D: Data Protection and Privacy Policy.

5. POLICY PRINCIPLES RELATING TO DATA BREACH

5.1 General Principles

5.1.1 Data Breaches are viewed seriously as they may expose the GPF to significant financial and reputational risks.

5.1.2 The business operations of the GPF must be conducted in such a manner as to comply with POPIA, GDPR (where applicable) and all policies relevant to privacy and data protection in order to prevent Data Breaches.

5.1.3 The GPF must continually understand and assess areas of weakness within its operating processes and continuously improve these in order to reduce the risk of significant control failures leading to Data Breaches.

5.1.4 Adequate measures must be put in place to prevent instances that may lead to Data Breaches. These instances include, without limitation:

a) loss or theft of data or equipment on which Personal Information is stored;

b) inappropriate access controls allowing unauthorized use;

c) equipment failure;

d) human error (which includes theft or loss of GPF documentation, Personal Information emailed or posted to an incorrect recipient, failure to redact Personal Information, responding to emails through which malware is installed on the Employee's computer, etc.)

e) unforeseen circumstances, such as fire or flood;

f) deliberate attacks on systems, such as hacking, viruses, or phishing scams; and/or

g) alteration of Personal Information without permission and loss of availability of Personal Information.

5.1.5 Adequate measures and structures must be put in place to contain and remediate Data Breaches timeously and effectively.

5.1.6 Where Data Breaches occur or are believed to have occurred, they must be identified and reported quickly and effectively within established measures and structures to limit any impact on business.

5.1.7 Actions to address Data Breaches must be proportionate, consistent, and transparent.

5.1.8 Data Breaches must be addressed in a timely, systematic, and orderly manner in order to effectively manage any risk to both the GPF and the affected Data Subjects.

5.1.9 Post-breach reviews must be undertaken to assess the effectiveness of this Policy and make enhancements to prevent reoccurrence of Data Breaches.

5.1.10 The duty to ensure compliance with all privacy and data protection laws and policies does not exclusively reside with the Information Officer. All Personnel share the responsibility to ensure compliance with such laws and policies and to take all steps and actions to contain and remedy Data Breaches.

5.2 Data Breaches reporting structure

5.2.1 The Information Officer is primarily and responsible for receiving reports of any Data Breaches and the implementation of this Policy.

5.2.2 Together with the Information Officer, the Response Team is responsible for timeously assessing any potential, suspected or actual Data Breaches (including the cause thereof, the Personal Information involved (how sensitive the information is) and how the Data Breach occurred) and responding to such Data breaches with the necessary expertise. The GPF shall, from time to time, appoint such Employees as it deems appropriate to competently discharge the responsibilities of the Response Team.

5.2.3 The Exco is responsible for receiving from the Information Officer, any reports of Data Breaches deemed serious and in consultation with the Information Officer, reporting such Data Breaches, risk, and remedial measures to the ARC.

5.2.4 The ARC is responsible for exercising oversight over the implementation of this Policy, including implementation and effectiveness of measures to prevent, mitigate or remedy Data Breaches reported to it by Exco, in consultation with the Information Officer.

5.2.5 Internal Audit is responsible for monitoring and auditing compliance with this Policy as well as making recommendations on the implementation of the Policy.

5.2.6 All Personnel, contractors, consultants, advisors, and service providers of the GPF that may deal with its Personal Information are responsible for reporting any actual, suspected, or potential Data Breaches to the Information Officer.

5.3 Reporting Data Breaches

5.3.1 All known or reasonably suspected actual or potential Data Breaches must be reported in writing by the person who knows or suspects such Data Breach.

5.3.2 The Information Officer must take appropriate steps to deal with the report in collaboration with the Response Team.

5.3.3 Data Breaches deemed serious by the Information Officer must also be reported to Exco and the ARC.

5.4 Investigation, management, containment and recording of Data Breaches

5.4.1 All reported Data Breaches must be formally investigated and addressed in a timely, expeditious, systematic, and orderly manner in order to effectively manage any risk to both the GPF and the affected Data Subjects.

5.4.2 The Information Officer in collaboration with the Response Team, must assess the Data Breach and its impact by:

(a) identifying how the Data Breach occurred and/or making an evidence-based evaluation as to the harm that has occurred or that may materialize from the Data Breach and the extent of repercussions of the Data Breach to both the GPF and Data Subjects;

(b) where possible, stopping the unauthorized activity immediately by taking steps to recover the data and/or limit any further dissemination, destruction, and access to the affected Personal Information;

(c) if necessary, timeously notifying the relevant cyber insurance provider in writing about the Data Breach; and

(d) recording the full details of the assessment of the Data Breach in writing.

5.4.3 The full details of all Data Breaches, their causes and remedial action must also be recorded by the Information Officer and Response Team in a Data Breach Log which must be maintained and regularly updated. The Data Breach Log must be made available to the Information Regulator when required.

5.4.4 All evidence relating to the investigation of a Data Breach must be appropriately preserved and all and any decisions made in relation to the Data Breach must be recorded.

5.5 Notifications of Data Breaches

5.5.1 All Data Breaches deemed serious by the Information Officer must be reported to Exco for onward reporting to ARC.

5.5.2 Data Breaches where it is reasonably believed that the Personal Information of a Data Subject has been accessed or acquired by an unauthorized person must be reported to the Information Regulator and the Data Subject (unless their identity cannot be established) in writing as soon as reasonably possible after the discovery of the Data Breach. Where the GDPR applies, the relevant European Union Supervisory Authority must be notified not later than 72 hours after acquiring knowledge of a Data Breach.

5.5.3 A notification to a Data Subject may be delayed where a public body responsible for the prevention, detection or investigation of offences or the Information Regulator finds that the notification will impede a criminal investigation by the relevant public body.

5.5.4 Notifications of Data Breaches in terms of contractual obligations must be conducted in the manner specified in the relevant contract.

5.6 Public communications of Data Breaches

The GPF must have a strategy to communicate with stakeholders in cases of Data Breaches that warrant publication and communication.

5.7 GPF acting as "operator" or "processor"

5.7.1 Where GPF acts as an 'operator' for purposes of POPIA and, where applicable, the GDPR (in which case it would act as a 'processor') and should any Data Breach affect the data of Data Subjects whose information the GPF processes as an operator, it shall notify the relevant responsible party (or 'controller') immediately where there are reasonable grounds to believe that the Personal Information of relevant Data Subjects has been accessed or acquired by any unauthorized person. The Information Officer will coordinate such communications.

5.8 Third parties acting as GPF's "operator" or "processor"

5.8.1 The relevant provisions of POPIA and GDPR as well as all the provisions of this Policy are equally applicable to third parties acting as operators or processors for the GPF, with the necessary adjustments required by context.

5.8.2 GPF's operators and processors must immediately inform the GPF (via the office of the Information Officer) of any Data Breaches. Any reports of such Data Breach to the Information Regulator and Data Subjects must be done in collaboration with the Information Officer.

6. BREACH OF POLICY

6.1. Breach of any clause contained in the policy shall be subjected to GPF disciplinary procedures without prejudice to any other rights that GPF may have in law to recover any damages suffered as a result of such non-compliance.

6.2. If any Employee does not understand sections, descriptions or concepts contained within this document, it is the responsibility of the individual to obtain clarity.

7. MONITORING, REVIEW AND COMPLIANCE

7.1. Policy Audit

The Information Officer and/or the Deputy Information Officer shall report on the progress and specific problems experienced in the implementation thereof.

7.2. Policy Review

This Policy is subject to review on an annual basis or as and when the need may arise.

7.3. Policy amendments

No amendment (s) may be made to any section(s) of this policy without such amendment (s) first being discussed and validated against prevailing acts, standards, best practices, and regulations by the Policy Owner supported by Exco and ARC.

7.4. Policy Compliance

The Legal and Compliance Unit will play a monitoring and evaluation role to determine whether the approved policy provisions will provide compliance assurance and determine whether the approved policy provisions are put in place in each Business Unit within GPF as well as ensure legislative compliance.

8. APPROVAL

This policy is approved by the Board after consideration and recommendation from Exco and ARC.