Khuseti HOLDINGS

DATA BREACH POLICY	
Classification	POPIA / 02
Responsible person	Information Officer / deputy information officers
Version	2021/06
Review date	2022/06
Guideline documents	Werksmans Attorneys
Author	Nawhal Kock
CEO Approval	**Andre Els**
Signature	

1 **PURPOSE**

1.1 To outline the process for notifying affected individuals of a privacy breach in terms of the Protection of Personal Information Act, 2013 ("**POPIA**").

1.2 It is essential for all staff to comply with this policy – Security compromises must be notified to the Regulator and to the affected individuals.

2 **SCOPE**

2.1 This policy applies to all staff, which includes all permanent and temporary staff and contractors.

2.2 Failure to comply may lead to disciplinary action, including summary dismissal (without notice or a payment in lieu of notice) or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

3 **DEFINITIONS**

3.1 **Breach** – Unauthorised acquisition, access, use, or disclosure or reasonable belief of unauthorised acquisition, access, use or disclosure of Personal Information that comprises the security, confidentiality, or integrity of the Personal Information.

3.2 **Personal Information** – Personal Information as defined in POPIA and includes all information in terms of which an individual or company can be identified.

4 **KEY CONSIDERATIONS**

4.1 Has to comply with POPI to ensure that measures are taken to keep data secure, including specific legal obligations around dealing with a security compromise. Such legal requirements must be observed in addition to the approach set out in this policy.

4.2 This policy includes guidelines on how to deal with security compromises, including:

4.2.1 containment and initial assessment;

5 **RISK EVALUATION;**

5.1.1 breach notification;

5.1.2 remedial action; and

5.1.3 Incident response plan.

6 **PROCEDURE**

6.1 **Reporting a Possible Breach**

6.1.1 Any employee who becomes aware of a possible breach of privacy involving Personal Information in the custody or control of will immediately inform their supervisor/manager, and the Information Officer.

6.1.2 Notification should occur immediately upon discovery of a possible breach.

6.1.3 The supervisor/manager will verify the circumstances of the possible breach and inform the Information Officer and or the Deputy Information Officers.

6.1.4 You may call the Information Officer directly at **011 564 9701 and or 082 770 4494**.

6.1.5 You are required to provide the Information Officer with:

6.1.5.1 As much detail as possible in relation to the Breach.

6.1.5.2 Provide the Information Officer with as much detail as possible.

6.1.5.3 Be responsive to requests for additional information from the Information Officer.

6.1.5.4 Be aware that the Information Officer has an obligation to follow up on any reasonable belief that Personal Information of PPI has been compromised.

6.1.6 Confidentiality: The information officer and deputy information officers should also consider keeping the investigation confidential from those (internally or externally) that do not need to be made aware of the investigation (either wholly or in part). This will allow the investigation to continue

Unhindered particularly with regard to further scoping of the incident and any activity around it. This may include, for example, notifying an appropriate law enforcement authority.

6.1.7 See **Annexure A** for a Breach Incident Report Template.

6.2 **Containing the Breach**

The Information Officer will take the following steps to limit the scope and effect of the breach.

6.2.1 Work with department(s) to immediately contain the breach. Examples include, but are not limited to:

6.2.1.1 Stopping the unauthorised practice;

6.2.1.2 Recovering the records, if possible;

6.2.1.3 Shutting down the system that was breached;

6.2.1.4 Mitigating the breach, if possible;

6.2.1.5 Correcting weaknesses in security practices; and

6.2.1.6 Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity.

6.2.2 Investigating and Evaluation the Risks Associated with the Breach:

6.2.2.1 To determine what other steps are immediately necessary, the Information Officer in collaboration with the Deputy Information Officers and affected department(s), will investigate the circumstances of the breach.

6.2.2.2 The "Team" meaning the Information officer together with the Deputy Information Officers will review the results of the investigation to determine root cause(s), evaluate risks, and develop a resolution plan.

6.2.2.3 The Privacy Breach Assessment Tool will help aid the investigation. See **Annexure B** for the template document.

6.2.3 The Information Officer, in collaboration with the Deputy Information officers, will consider several factors in determining the notifications to individuals affected by the breach including but not limited to:

6.2.3.1 Contractual obligations;

6.2.3.2 Risk of identity theft or fraud because of the type of information lost such as contact details, banking information, identification numbers);

6.2.3.3 Risk of physical harm if the loss puts an individual at risk of stalking or harassment);

6.2.3.4 Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records; and

6.2.3.5 Number of individuals affect

6.3 **Notification**

6.3.1 The Information Officer with the Deputy Information Officers will work with the department(s) involved, to decide the best approach for notification and to determine what may be required by law.

6.3.2 Notification of the Information Regulator will occur as soon as possible following the breach The Information Regulator

6.3.3 Notification of individuals affected by the breach will occur as soon as possible following the breach.

6.3.4 Affected individuals must be notified without reasonable delay, unless such notification will impair a criminal investigation.

6.3.5 Notices must be in plain language and include basic information, including:

6.3.5.1 What happened;

6.3.5.2 Types of PI involved;

6.3.5.3 Steps individuals should take;

6.3.5.4 Steps being taken; and

6.3.5.5 Contact Information.

6.3.6 Notices should be sent by mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.

6.3.7 If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.

6.3.8 The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Information Officer and Deputy Information Officers should work closely to draft any notification that is distributed.

6.3.9 Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.

6.3.10 Using multiple methods of notification in certain cases may be the most effective approach.

6.4 Prevention

6.4.1 Once immediate steps are taken to mitigate the risks associated with the breach, the Information Officer and Deputy Information Officers will investigate the cause of the breach.

6.4.2 If necessary, this will include a security audit of physical, organisational, and technological measures.

6.4.3 This may also include a review of any mitigating steps taken.

6.4.4 The Information Officer and Deputy Information Officers will assist the responsible department to put into effect adequate safeguards against further breaches.

6.4.5 Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.

6.4.6 The resulting plan will also include audit recommendations, if appropriate.

6.4.7 See **Annexure C** for a Breach Incident Investigation Report Template.

7 COMPLIANCE AND ENFORCEMENT

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination.

8 CONTACT DETAILS OF THE INFORMATION OFFICER AND DEPUTY INFORMATION OFFICERS

8.1 Name: **Andre Els**

8.2 Address: **807 Richards Drive, Eastside Corporate Close, Midrand, 1635**

8.3 E-mail address: **ElsFA@kingpie.co.za**

8.4 Telephone number: **011 564 9701**

Deputy information Officer	**Deputy information Officer**
Legal & Commercial Executive: Renier Bouwer	**CFO**: Mohammed Matwadia
Telephone number: (011) 564 9701 Email address: bouwerr@kingpie.co.za	Telephone number: (011) 564 9701 Email address: Matwadiam@kingpie.co.za
Deputy information Officer	**Deputy information Officer**
Human Resource Manager: Nawhal Kock	**Operations Executive**: Dewald De Vos
Telephone number: (011) 564 9701 Email address: KockN@kingpie.co.za	Telephone number: (011) 564 9701 Email address: devosd@kingpie.co.za

Deputy information Officer	**Deputy information Officer**
Marketing Manager: Nodumo Novuka	**National Sales Manager**: Kuvesh Budhoo
Telephone number: (011) 564 9701 Email address: NovukaN@kingpie.co.za	Telephone number: (011) 564 9701 Email address: BudhooK@bmofoods.co.za
Deputy information Officer	
Marketing Manager: Kagiso Lehari	
Telephone number: (011) 564 9701 Email address: LehariK@bmofoods.co.za	

ANNEXURE A

BREACH INCIDENT REPORT

Directions: The reporting employee or witness needs to complete Section 1 and Section 2. If needed, the employee or witness can consult with the IT Department to complete Section 2. **Please Note:** All persons who contribute information to the report should be recorded in the "Report Augmented By" field. When completed, the form should be **submitted to the Information Officer** with a copy to be retained by the reporting employee or witness and, if applicable, to be provided to the employee's Supervisor. Please print clearly.

Section 1: Incident Reporter			
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			
(If Available) Alternate Phone Number:			
Report Submitted To – **Indicate name and title:**			
Section 2: Incident Details			
Date and Time of Discovery of Incident:		Estimated Date and Time Incident Started:	
Description of Incident – **Be Specific:**			
PI Compromise Suspected?	☐ Yes ☐ No		
Location of Incident:			
Current Status of Incident:			
Source or Cause of Incident:			
Employees, Contractors or Others with Incident Knowledge – **List all known potential witnesses:**			

Operating System, version, and patch level:	
Antivirus Software Installed, Enabled and Updated?	☐ Yes ☐ No Comments:
Description of Affected Resources:	
Mitigating Factors:	
Estimated Technical Impact of Incident:	
Response Actions Performed:	
Other Organisations Contacted:	
Report Augmented By:	
Additional Comments:	

I understand that by submitting this Incident Report in good faith, I cannot be subject to retaliation. I attest that the information contained in this Incident Report is true and accurate to the best of my knowledge on the date indicated below. If I obtain any additional information regarding this incident, I agree to provide said supplementary information to the person specified above in "Report Submitted To" and/or the designated Incident Handler. I agree to cooperate fully with all investigators of this incident until the incident is closed.

_____ _____

Incident Reporter's Signature Date

Khuseti HOLDINGS

ANNEXURE B

PRIVACY BREACH ASSESSMENT

1 **Was Private Information Involved?**

☐ Yes ☐ No

2 **Was the Private Information encrypted?**

☐ Yes ☐ No

3 **Description of breach:**

3.1 What data elements have been breached? Identification numbers, contact details, financial information that could be used for identity theft are examples of sensitive personal information.

3.2 What possible use is there for the private information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

3.3 What was the date that the breach was discovered? _____

3.4 What is believed to be the date that the breach occurred? _____

4 **Cause and Extent of the Breach**

4.1 What is the cause of the breach?

4.2 Is there a risk of ongoing or further exposure of the information?

☐ Yes ☐ No

4.3 What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?

4.4 Is the information encrypted or otherwise not readily accessible?

☐ Yes ☐ No

4.5 What steps have already been taken to minimize the harm?

5 Individuals Affected by the Breach

5.1.1 How many individuals are affected by the breach? _____

5.1.2 Who was affected by the breach:

☐ Employees

☐ Customers

☐ Volunteers

☐ Contractors

☐ Service providers

☐ Other individuals/organizations

6 Foreseeable Harm from the Breach

6.1 Is there any relationship between the unauthorized recipients and the data subject?

☐ Yes ☐ No

6.2 Is any of the information or the individual whose information was compromised subject to additional protections, such as court orders, temporary restraining orders, protections from harm, etc.?

6.3 What harm to the individuals will result from the breach? Harm that may occur includes:

- ☐ Security risk (e.g., physical safety)
- ☐ Identity theft or fraud
- ☐ Loss of business or employment opportunities
- ☐ Hurt, humiliation, damage to reputation or relationships
- ☐ Other (please specify):

6.4 What harm could result to the organisation as a result of the breach?

- ☐ Loss of trust in the organisation
- ☐ Loss of assets
- ☐ Financial exposure
- ☐ Other (please specify):

6.5 What harm could result to the public as a result of the breach?

- ☐ Risk to public health
- ☐ Risk to public safety
- ☐ Other (please specify):

7 Privacy Analysis

7.1 Determine if the incident poses a risk to individuals. The following factors shall be considered when assessing the likely risk of harm and level of impact for a potential or confirmed privacy breach-

7.1.1 Nature of the data elements breached in light of their context and the broad range of potential harms that may result from their disclosure to unauthorised individuals;

7.1.2 Potential harm to reputation of individuals;

7.1.3 Potential for harassment or prejudice;

7.1.4 Potential for identity theft, including any evidence that breached information is actually being used;

7.1.5 Number of individuals affected;

7.1.6 Likelihood that breach was the result of a criminal act or will result in criminal activity;

7.1.7 Likelihood the information is accessible and usable by unauthorized individuals;

7.1.8 Likelihood the breach may lead to harm; and

7.1.9 Ability to mitigate the risk of harm.

7.2 If an identity theft risk is present, tailor the response to the nature and scope of the risk presented. Notice may not be required in all circumstances, so the response team should assess the situation and determine if notification to individuals is necessary. In some cases, notification may actually increase a risk of harm, in which case should delay notification until proper safeguards can be instituted. The analysis of whether notification is necessary should be based on the following factors –

7.2.1 Urgency with which individuals need to receive notice;

7.2.2 Whether other public and private sector agencies need notification, particularly those that may be affected or may play a role in mitigating the breach;

7.2.3 Contact information available for affected individuals; and

7.2.4 Whether media outlets may be the best way to alert affected individuals and mitigate any risk.

7.3 Written notification should include the following elements -

7.3.1 Brief description of what happened, including the date of the breach and its discovery;

7.3.2 Description of the types of information involved in the breach;

7.3.3 Statement whether the information was protected, if such information would be beneficial and would not compromise security;

7.3.4 Steps individuals should take to protect themselves from harm;

7.3.5 What is doing to investigate and mitigate the breach; and

7.3.6 Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address and postal address.

7.4 If the response team determines that public notification through the media is necessary, it should also post notification of the breach on its website, with the same information required for written notification to the individual. The posting should provide answers to frequently asked questions and other talking points.

8 **Breach Analysis Follow-Up**

Once the breach analysis is complete and notice is provided, should review policies, procedures and security measures to incorporate any necessary updates or changes.

Khuseti
HOLDINGS

ANNEXURE C

BREACH INCIDENT INVESTIGATION REPORT

Directions - Upon receipt of a Breach Incident Report, an investigation into the incident shall be initiated. The Breach Incident Investigation Report should be completed as thoroughly as possible by the Incident Handler and Investigators. Since investigations vary, some sections may not be applicable to every investigation. In the electronic version, clicking on any blue link in the form will move you to the applicable instructions.

Section 1: Incident Handler			
Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, extension:			

Section 2: Incident Update	
Current Status of Incident Response:	
Summary of Incident:	

Section 3: Investigators				
Name	**Title**	**Organisation**	**Phone**	**Email**

Section 4: Log of Actions Taken			
Date	**Incident Handler/ Investigator**	**Action**	**Results**

Section 5: Evidence Found		
Date	**Incident Handler/ Investigator**	**Evidence**

Section 6: Parties Involved in Incident				
Name	**Title**	**Organization**	**Phone**	**Email**

Section 7: Incident Handler and Investigator Comments		
Date	**Incident Handler/ Investigator**	**Comments**

Section 8: Findings		
Type of Incident:	☐ Unauthorised Access	☐ Inappropriate Usage
☐ Malicious Code	☐ Denial of Service	☐ Multiple Component
Cause of Incident:		
Cost of Incident:		
Business Impact of Incident:		

PHI Compromised? ☐ Yes ☐ No

If yes, Estimated Number of Compromised PI Accounts: _____ - or -

(If known) Actual Number of Compromised PI Accounts: _____.

PHI Breach Impact: ☐ High (≥ 500 PI Accounts) ☐ Medium (< 500 PI Accounts) ☐ Unknown

Data Encrypted? ☐ Yes ☐ No If yes, description of encryption:_____.

Important Note: If PI accounts may have been compromised and data was not encrypted, please follow breach evaluation procedures and, if necessary, breach notification procedures.

Was the breach evaluation processes initiated? ☐ Yes ☐ No

If yes, date of breach evaluation initiation: _____.

Section 9: Recommended Corrective Actions		
Recommended By	**Date**	**Recommended Corrective Action**

Section 10: Actions Taken		
Performed By	**Date**	**Action Taken**

Section 11: Notifications Made			
Organisation	**Point of Contact**	**Date of Notification**	**Summary of Information Provided**

I attest that the information contained in this Investigation Report is true and accurate to the best of my knowledge and the knowledge of all contributors. I further attest that all parties who participated in the investigation, all findings of the investigation, and all recommended corrective actions as well as all actions taken by any parties to this investigation are clearly documented. This

Investigation Report has been provided to the Information Officer for review in both its final form and, as appropriate, throughout the term of the investigation. Effective on the date indicated below, this incident investigation is considered closed.

_____ _____

Incident Handler's Signature Date