HAZCHEMWIZE
Strategic Solutions for Dangerous Goods

Hazchemwize (Pty) Ltd
T/A HAZCHEMWIZE (PTY) LTD
REGISTRATION NUMBER: 2002/020331/07

DATA BREACH NOTIFICATION POLICY

REGULATION 4

OF PROTECTION OF PERSONAL INFORMATION ACT 2013

1. INTRODUCTION

The PoPI Act aims to protect the Rights of individuals about whom Data is obtained, stored, processed or supplied and requires that Responsible Party takes appropriate Security Measures against unauthorised access, alteration, disclosure or destruction of Personal Information and Data of Hazchemwize (Pty) Ltd.

The PoPI Act places obligations on Employees to report actual or suspected Data Breaches and our procedure for dealing with breaches is set out below. All Employees are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all Employees to enable them to carry out their obligations within this Policy.

Data Processors will be provided with a copy of this Policy and will be required to notify Hazchemwize (Pty) Ltd of any Data Breach without undue delay after becoming aware of the Data Breach. Failure to do so may result in a breach to the terms of the Processing Agreement.

Breach of this Policy will be treated as a disciplinary offence which may result in disciplinary action under Hazchemwize (Pty) Ltd's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the Data Breach.

This Policy does not form part of any individual's terms and conditions of employment with Hazchemwize (Pty) Ltd and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this Policy in order to remain compliant with legal obligations.

2. RESPONSIBILITY

The Information Officer has overall responsibility for breach notification within Hazchemwize (Pty) Ltd. They are responsible for ensuring breach notification processes are adhered to by all Employees and are the designated point of contact for Personal Data Breaches.

In the absence of the Information Officer, please contact the Office Manager / Compliance Officer of Hazchemwize (Pty) Ltd.

The Information Officer is responsible for overseeing this Policy and developing Data-related Policies and Guidelines.

Please contact the Information Officer with any questions about the operation of this Policy or the PoPI Act or if you have any concerns that this Policy is not being or has not been followed.

The Information Officer's contact details are set at the end of this document.

3. DATA PROTECTION POLICY (INFORMATION SECURITY POLICY)

Employees should refer to the following Policies that are related to this Data Protection Policy (Information Security Policy):

- Privacy Policy which sets out Hazchemwize (Pty) Ltd's obligations under the PoPI Act about how they process Personal Data and includes Hazchemwize (Pty) Ltd's Security Policy which sets out Hazchemwize (Pty) Ltd's Guidelines and Processes on keeping Personal Data secure against loss and misuse.

These Policies are also designed to protect Personal Data and can also be found in Hazchemwize (Pty) Ltd's Privacy Policy and Statement.

4. A PERSONAL DATA BREACH

A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data or Special Category Data transmitted, stored or otherwise processed.

Examples of a data breach could include the following, but are not exhaustive:

- Loss or theft of data or equipment on which Data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an e-mail or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where Information is obtained by deceiving whoever holds it.

5. REPORTING A DATA BREACH

Hazchemwize (Pty) Ltd must notify the Information Officer of a Data Breach where it is likely to result in a risk to the Rights and freedoms of individuals. This means that the breach needs to be more than just losing Personal Data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the Breach may have a significant Effect includes:

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the Rights and freedoms of individuals then the individuals must also be notified directly.

6. MANAGING AND RECORDING THE BREACH

On being notified of a suspected Personal Data Breach, the Information Officer will take immediate steps to establish whether a Personal Data Breach has in fact occurred. If so they will take steps to:

- Where possible, contain the Data Breach;
- As far as possible, recover, rectify or delete the Data that has been lost, damaged or disclosed;
- Assess and record the breach in Hazchemwize (Pty) Ltd's Data Breach Register;
- Notify the Information Regulator;
- Notify Data Subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

7. NOTIFYING THE INFORMATION REGULATOR

The Information Officer will notify the Information Regulator when a Personal Data Breach has occurred which is likely to result in a risk to the Rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. If Hazchemwize (Pty) Ltd is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the Information Regulator.

8. NOTIFYING DATA SUBJECTS

Where the Data Breach is likely to result in a high risk to the Rights and freedoms of Data Subjects, the Human Resources Director will notify the affected individuals without undue delay including the name and contact details of the Information Officer and Information Regulator, the likely consequences of the Data Breach and the measures Hazchemwize (Pty) Ltd has or intends to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, Management will co-operate with and seek guidance from the Information Officer, the Information Regulator and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the Data Subjects directly (for example, by not having contact details of the affected individual) then Hazchemwize (Pty) Ltd will consider alternative means to make those affected aware for example by making a statement on Hazchemwize (Pty) Ltd's website.

9. NOTIFYING OTHER AUTHORITIES

Hazchemwize (Pty) Ltd will need to consider whether other parties need to be notified of the breach.

For example:

- Insurers;
- Parents;
- Third Parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

10. ASSESSING the Breach

Once initial reporting procedures have been carried out, Hazchemwize (Pty) Ltd will carry out all necessary investigations into the breach.

Hazchemwize (Pty) Ltd will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of Personal Data. We will identify ways to recover correct or delete data, for example notifying our insurers or the police if the breach involves stolen hardware or data.

Having dealt with containing the breach, Hazchemwize (Pty) Ltd will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken, for example notifying the Information Regulator and/or Data Subjects as set out above.

These factors include:

- What type of Data is involved and how sensitive it is;
- The volume of Data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected Data Subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the Data (for example, encryption, password protection, pseudonymisation);
- What has happened to the Data;
- What could the data tell a Third Party about the Data Subject;
- What are the likely consequences of the Personal Data Breach on Hazchemwize (Pty) Ltd and
- Any other wider consequences which may be applicable.

11. PREVENTING Future Breaches

Once the Data Breach has been dealt with, Hazchemwize (Pty) Ltd will consider its security processes with the aim of preventing further breaches. In order to do this, we will:

- Establish what Security Measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate Employee awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether its necessary to conduct a Privacy or Data Protection Impact Assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the Data Breach Register;
- To debrief management following the investigation.

12. REPORTING DATA PROTECTION CONCERNS

Prevention is always better than dealing with Data Protection as an after-thought. Data Security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the Information Officer. This can help capture risks as they emerge and protect Hazchemwize (Pty) Ltd from Data Breaches and keep our processes up to date and effective.

13. MONITORING

We will monitor the effectiveness of this and all of our Policies and Procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our Policies and Procedures are working in practice to reduce the risks posed to Hazchemwize (Pty) Ltd.

14. REPORTING A Data Breach

If you know or suspect a Personal Data Breach has occurred or may occur which meets the criteria above, you should:

Complete a Data Breach Report Form (PoPI Incident Event Notification Form), which can be obtained from the Information Officer of Hazchemwize (Pty) Ltd (refer to Section 6.9 of this PoPI Manual).

E-mail the completed form to the Information Officer.

Where appropriate, you should liaise with Management about completion of the Data Report Form.

Breach reporting is encouraged throughout Hazchemwize (Pty) Ltd and Personnel are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the Rights and freedom of individuals.

They can seek advice from Information Officer.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Information Officer will acknowledge receipt of the Data Breach Report Form (PoPI Incident Event Notification Form) and take appropriate steps to deal with the Report.

15. CHANGES IN THIS POLICY

Hazchemwize (Pty) Ltd reserves the right to amend, alter and terminate this Policy at any time.

INFORMATION OFFICER DETAILS

IO Registration Number: 2024-003864

Name: Marce' Clare Joan Maneveldt

Tel: (011) 975-1278

Cell: 0823348870

Physical Address: 10 Zurich Road
Spartan
Kempton Park
1620

Date: 21 July 2025

Email: marcem@hazchemwize.co.za

Website: www.hazchemwize.co.za

Postal Address: P.O. Box 10122
Edleen
1619