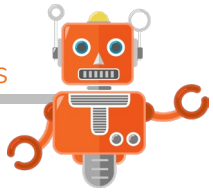

Data Breach Policy

TECHTRON COMPUTERS (PTY) LTD

Business Name

(Referred to as "The Business")

Contents

CONTENTS

1 Background 2

2 Aim 2

3 Definition 2

4 Scope 3

5 Responsibilities 3

6 Reporting a Breach Internal 4

7 Data Breach Management Plan 4

8 Disciplinary 4

9 Review 5

Prepared By:	Steven Sher
Date:	1st June 2021
Version:	1.3

1 BACKGROUND

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. The Business needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

2 AIM

The aim of this policy is to standardise the company's response to any data breach and ensure that

they are appropriately logged and managed in accordance with the law and best practice, so that:

- incidents are reported swiftly and can be properly investigated
- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further damage
- the regulator and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

3 DEFINITION

Act, No. 4 of 2013(POPIA) section 22 of POPIA provides that:

"(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unathorised person, the responsible party, must notify –

(a) The Regulator; and
(b) Subject to subsection (3), the data subject, unless the identity of such data subject cannot be established"

The Company is obliged under POPIA to act in respect of such data breaches. This procedure sets out how the Company will manage a report of a suspected data security breach.

The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

A data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy

- Data posted, e-mailed, or faxed to the incorrect recipient
- Loss or theft of equipment on which data is stored
- inappropriate sharing or dissemination-Staff accessing information to which they are not entitled
- Hacking, malware, data corruption
- Information is obtained by deception or “blagging”
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

In any situation where staff are uncertain whether an incident constitutes a breach of security, report it to the Information Officer(IO). If there are IT issues, such as the security of the network being compromised, IT should be informed immediately.

4 SCOPE

This Company-wide policy applies to all Company and information, regardless of format, and is applicable to all officers, members, visitors, contractors, partner organisations and data processors acting on behalf of the Company. It is to be read in conjunction with the Company’s other related Policy’s.

5 RESPONSIBILITIES

Information users

POPIA applies to both Data Controllers (the Company itself) and to Data Handlers. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers

Heads of Department are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

The Information Officer

Lead responsible officers will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable further delegation may be appropriate in some circumstances.

6 REPORTING A BREACH INTERNAL

Suspected data security breaches should be reported promptly to the Information Officer as the primary point of contact on 021 673 6756, email: info@techtron.co.za

The report must contain full and accurate details of the incident including who is reporting the incident [and what classification of data is involved]. The incident report form should be completed as part of the reporting process. See Appendix 1. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach.

All data security breaches will be centrally logged by the Information Officer to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

External

You will also be required to inform all the data subjects whose data has been compromised (unless the identity if such data subjects cannot be established), as well as the Information Regulator, as soon as reasonably possible after you become aware of the data breach.

A report to the Regulator must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of Information Officer, likely consequences of the breach and action taken.

7 DATA BREACH MANAGEMENT PLAN

The Company's response to any reported data security breach will involve the following four elements.

A. Containment and Recovery

B. Assessment of Risks

C. Consideration of Further Notification

D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist. An activity log recording the timeline of the incident management should also be completed.

8 DISCIPLINARY

Officers, members, contractors, visitors, or partner organisations who act in breach of this policy may

be subject to disciplinary procedures or other appropriate sanctions.

9 REVIEW

This document shall be subject to annual review by the Information Officer.

Appendix 1 Data Breach Reporting Template

	Report by:	**Name: Job Title:** **Service:** **Date:**
1.	Summary of event and circumstances	*Who, what, when, who etc.*
2.	Type and amount of personal data	*Title of document(s)-what information is included-name, contact details, financial, sensitive or special category data.*
3.	Action taken by recipient	
4.	Action taken to retrieve data and respond to breach	
5.	Procedure/policy in place to minimise risk	*Communication, secure storage, sharing, exchange.*
6.	Breach of policy/procedure by officer/member	*Has there been a breach of policy and has appropriate management action been taken?*
7.	Details of notification to data subject. Complaint received?	*Has data subject been notified? If not, explain why. What advice has been offered?*
8.	Details of Data Protection training provided.	*Date of most recent training by staff/ councillor involved*
9.	Risk assessment and changes need to prevent further data loss	
10.	Conclusions and learning points	