Pirtek Africa (Pty) Ltd

DATA BREACH AND INCIDENTS RESPONSE PLAN

2021

INTERNAL DATA BREACH AND INCIDENTS RESPONSE PLAN

NOTICE: THIS PLAN IS FOR INTERNAL USE ONLY AND IS NOT AVAILABLE FOR DISTRIBUTION TO THE PUBLIC WITHOUT PRIOR APPROVAL OF THE INFORMATION OFFICER OF THE COMPANY.

1. OVERVIEW

1.1. This plan aims to provide a foundation for the implementation of a practical response to data breaches and data security related incidents (this/the "**Plan**") depicting the internal procedures of the Company as required in terms of the Protection of Personal Information Act 4 of 2013 ("**POPIA/ the Act**"), should an Incident occur.

1.2. The focus of this Plan is to ensure that the provisions of POPIA are complied with should an Incident occur and that any interruption of the business of the Company is minimal and that continuity of the business activities is achieved as soon as is reasonably possible after such Incident.

1.3. Though reference to a number of data security related incidents is included in this Plan, it is specifically tailored to ensure compliance with the provisions of the Act.

1.4. The Practical Steps (as detailed in paragraph 4 below), aim to set out the obligations, applicable procedures and time frames for reporting and managing any Incident for every professional, manager and support staff member who is employed by the Company.

1.5. This Plan must be read together with any and all other documents, manuals and guidance documents of the Company pertaining to POPIA, and specifically the Data Protection Policy of the Company.

2. DEFINITIONS

In this document, unless the context otherwise requires, the following capitalised terms shall have the meanings assigned to them below and cognate expressions shall have corresponding meanings:

"**Company**"	means Pirtek Africa (Pty) Ltd, registration number 1998/022734/07;
"**Data Subject**"	means the person to whom Personal Information relates and is therefore the party whose Personal

	Information is Processed by Responsible Parties. Data Subjects include identifiable, living natural persons and if applicable, an identifiable existing juristic person, to whom Personal Information may relate;
"**Data Breach**"	means any unauthorized access to, or damage or destruction of the Personal Information of Data Subjects being Processed by the Company or an Operator engaged by the Company from time to time (as the context and relevant circumstances may require);
"**Employee(s)**"	any person who is employed by the Company from time to time and who is under an obligation to comply with the provisions of the Act and who may engage in or facilitate the Processing of Personal Information;
"**Incident(s)**"	means any Data Breach and any of the scenarios set out in paragraph 4 below, but is not limited to these, due to the constant changing dynamic of the workplace and society at large, as well as the evolution of risks;
"**Information Officer**"	means the individual from time to time who will be responsible, within the Company, for ensuring compliance with POPIA and being responsible for the governance, management and security of Personal Information, as required in terms of POPIA and as more comprehensively defined in the Act, and any reference to "**Information Officer**" shall also constitute a reference to a duly appointed "**deputy information officer**" as contemplated in terms of POPIA;
"**Information Regulator**"	means the statutory body that is responsible for the enforcement and implementation of POPIA and which has been bestowed with extensive powers in terms of the Act, including the power to receive and investigate complaints, impose sanctions and publish guidelines and guidance documents in terms of POPIA compliance requirements;
"**Line Manager**"	means the line manager of any particular Employee of the Company;

"**Personal Information**"	any information relating to a Data Subject, and which includes general Personal Information and Special Personal Information (as the relevant context and circumstances may require);
"**POPIA / the Act**"	the Protection of Personal Information Act 4 of 2013, as amended from time to time;
"**Practical Steps**"	the framework established by this Data Breach and Incidents Response Plan of the Company and detailed in paragraph 4, and which is aimed at ensuring that in cases where a Data Breach has occurred or a potential Data Breach is identified that all Employees know which procedures to follow;
"**Processing**"	the processing of Personal Information involves any collection, use, storage, deletion or destruction of Personal Information. The processing of Personal Information is of an ongoing nature and compliance with the provisions of POPIA must be in place for as long as the Personal Information is being processed and stored, and "**Process**" and "**Processed**" in this context shall have a corresponding meaning;
"**Senior Management**"	the board of directors of the Company from time to time;
"**Special Personal Information**"	means Personal Information concerning – (i) the religious or philosophical beliefs; (ii) race or ethnic origin; (iii) trade union membership; (iv) political persuasion; (v) health or sex life; or (vi) biometric information (which includes information that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition),

of a Data Subject; or

(vii) the criminal behaviour of a Data Subject to the extent that such information relates to –

a. the alleged commission by a Data Subject of any offence; or

b. any proceedings in respect of any offence allegedly committed by a Data Subject or the disposal of such proceedings.

3. RISK IDENTIFICATION

3.1. For purposes of this Plan, an Incident will include both potential and actual Data Breaches. Although this does not necessarily constitute an exhaustive list, the scenarios as set out below depict risks relating to data security and the protection of Personal Information:

3.1.1. **Physical breaches**

3.1.1.1. Physical breaches (such as, but not limited to, break-ins, theft and/or destruction) of the Company's offices or assets (as the case may be in line with the relevant circumstances) involving the unauthorised access, theft, loss or destruction of Personal Information, such as a break-in during which physical files, mobile devices (including cell phones, laptops and wearables), storage devices (including SD cards, USB devices, external hard-drives and any other storage device) is either stolen, lost or destroyed.

3.1.1.2. It is important for Employees to keep in mind that theft or loss of Personal Information may not only occur as a result of a physical break in at the Company's offices. Any mobile device, including laptops and cell phones that are used to Process Personal Information, as well as physical files may be lost or stolen while under the control of an Employee outside of the Company's offices.

3.1.1.3. In cases where an Employee works from home, this may also extend to circumstances where the above occurs at their home or relevant off-site workplace.

3.1.2. **Electronic breaches**

3.1.2.1. Though the Company goes to great lengths to ensure that all Personal Information and data stored on our servers is secure and safe from unauthorised access and damage, no system is infallible. As such the risk of a systems failure remains a real possibility.

3.1.2.2. Electronic breaches (such as, but not limited to, virus infection, hacking, spyware) may be very difficult for most Employees to identify; however, it remains the responsibility of each employee to ensure that they comply with the cyber security policy of the Company.

3.1.2.3. It is the responsibility of every Employee to ensure that he/she remains vigilant against all threats and potential threats at all times, and that they keep themselves informed of potential new risks.

3.1.3. **Natural disasters**

Natural disasters (such as, but not limited to, fire, flood and power outages) may lead to the destruction or loss of Personal Information which is Processed at the Company's Offices. This also extends to employees working from home, or who Process Personal Information away from the Company's offices, who may be similarly affected.

3.1.4. **Technical errors, failures and malfunctions**

These include, but not are not limited to, hardware failures, as well as errors, failures and malfunctions in relation to servers, databases and networks, which have the potential to compromise the confidentiality of Personal Information, or the destruction or damage thereof.

3.1.5. **Accidents and unintended errors**

3.1.5.1. In light of the significant volume of Personal Information that is Processed by the Company, Employees must consistently be aware of and guard against the risk posed by human error.

3.1.5.2. Human error in the Processing of Personal Information may lead to the loss, deletion or accidental corruption of files, as well as potential unauthorised access of Personal Information or a compromise in the confidentiality thereof.

3.1.6. **Other disruptions**

3.1.6.1. Deliberate acts of sabotage or negligence (from either internal or external sources) may also lead to the loss or destruction of Personal Information Processed by the Company.

3.1.6.2. These may include the deletion of Personal Information from the servers and online platforms of the Company, as well as damage to physical files.

4. PRACTICAL STEPS

4.1. Although the Company takes all reasonable steps to secure and safeguard the Personal Information Processed by us, there is no guarantee that Incidents may not occur from time to time. When this inevitably happens, it is the duty of every Employee to ensure that he/she follows the necessary procedures as set out in this Plan, in order to ensure that potentially adverse consequences of an Incident are curbed or mitigated and that the Company is able to comply with its obligations under POPIA in these circumstances.

4.2. The following procedure should be followed and considerations taken into account in the event of an Incident:

4.2.1. **Reporting Disasters**

4.2.1.1. It is and remains the duty of any Employee that becomes aware of an Incident or potential Incident to report it, without delay, to the relevant person as identified within the Reporting Structure attached as “Annexure A” hereto.

4.2.1.2. Although no Incident should be disregarded or considered inconsequential, certain circumstances do give rise to a more urgent need for immediate action. In order to assist Employees to identify the appropriate time frame to report a disaster, the Time Frames for Reporting is attached as “Annexure B” hereto. These timeframes should be adhered to by all Employees, but as a rule Employees are obliged to make the necessary report as soon as they become aware of the Incident, or as soon as is reasonably possible thereafter.

4.2.2. **Impact Analysis**

4.2.2.1. Not all Incidents affect the business operations of the Company to the same extent, but the Company may have to comply with certain action steps in terms of POPIA when an Incident occurs.

4.2.2.2. In order to ensure that there is clarity on the likelihood as well as the impact of any Incident is likely to have on the Company, the assessment framework attached as “Annexure C” hereto may be used as guideline by Employees.

4.2.2.3. It is important for Employees to keep in mind that the impact which any Incident may have on the Company is determined by a variety of factors, including the severity and extent to which an Incident takes place. It is therefore important for all Incidents to be reported, in order for an impact analysis to be conducted.

4.2.3. **Incident response**

4.2.3.1. Subsequent to the determination of the type of Incident, the reporting thereof and the analysis conducted in relation to the impact that the Incident has on the business activities and POPIA responsibilities of the Company, Senior Management will determine the appropriate way forward and inform Employees accordingly.

4.2.3.2. Employees may be assigned a task or requested to perform certain actions, whether by their Line Manager, the Information Officer or Senior Management, if same is deemed an appropriate course of action.

5. CONFIDENTIALITY DUTIES OF EMPLOYEES

5.1. For the avoidance of any doubt, it is affirmed that all Employees of the Company are expected to keep this Plan, its contents and any actions taken in accordance with its provisions as confidential.

5.2. In addition to the above, any Incident that arises is to be treated with the utmost confidentiality in relation to third parties, in order to ensure that affected clients, suppliers, the general public and the Information Regulator are informed of the Incident in an appropriate manner, as Senior Management may determine in accordance with the relevant circumstances.

6. BREACH OF THE MEASURES SET OUT IN THIS PLAN

Any Employee who fails to comply with the provisions of this Plan may be subject to disciplinary action as a result of such failure, subject to a determination of the severity of the failure to comply and the consequences of such failure.

ANNEXURE A: REPORTING STRUCTURE

The table below sets out the reporting structure and depending on the position of the Employee that reports the Incident:

EMPLOYEE TO TAKE ACTION	PERSON/BODY TO WHOM THE EMPLOYEE MUST REPORT
Employee that identifies Incident	Line Manager
Line Manager	Information Officer
Information Officer	Senior Management

ANNEXURE B: TIME FRAMES FOR REPORTING DISASTERS

The table below sets out the appropriate time frames within which an Incident must be reported. However, it remains the duty of Employees to report an Incident as soon as they are able to do so and they should not wait for the time set out below to lapse prior to reporting it.

Incident	Employee to report to line manager within	Matter to escalate to
Physical breaches	As soon as Employee becomes aware	Information Officer; Senior Management
Electronic breaches	Immediately	Information Officer; IT Departments; Senior Management
Natural Disaster	As soon as Employee becomes aware	Information Officer; Senior Management
Technical errors, failures and malfunctions	Within 24 Hours	IT Departments; Senior Manager
Accidents and unintended errors	As soon as Employee becomes aware	IT Departments; Senior Manager
Other disruptions	As soon as Employee becomes aware	Line Manager to use discretion to determine severity of the matter

ANNEXURE C: IMPACT ANALYSIS

The below table provides examples of how severe each type of Incident may be, as well as to demonstrate that certain types of Incidents may have a low, medium or high impact depending on the circumstances:

LOW LEVEL IMPACT	MEDIUM LEVEL IMPACT	HIGH LEVEL IMPACT
Loss of Physical Hardware	Temporary failure of server access	Failure of servers with loss of Data
Loss of Municipal Power	Hardware Failures	Remote attacks on IT Systems
	Natural Disasters	Malicious disruptions
	Accidents	Physical Break Ins and theft
	Other disruptions	