RISK MANAGEMENT POLICY FOR THE OFFICE IN STELLENBOSCH PROPRIETARY LIMITED

("The Office" or "the company")

One of the important processing conditions of POPIA, is processing condition 7 that refers to security safeguards.

Section 19(2) of POPIA states:

(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
(a) loss of, damage to or unauthorised destruction of personal information; and
(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—
(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."

[POPI does not provide a "tick list" of security requirements to meet. Responsible parties must consider applicable

industry security practices and then implement security appropriate security measures for the business.]

Section 20 of POPIA states that:

An operator or anyone processing personal information on behalf of a responsible party or an operator, must—

(a) process such information only with the knowledge or authorisation of the responsible party; and

(b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties."

[This is the limitation on operators – they may not use personal information received from the responsible party for their own purposes outside of the scope of the contract with the responsible party.] – See Operator Agreement

Section 21 of POPIA states that:

(1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

[There is a duty on the responsible party to regulate the relationship with the operator by written contract.]

(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

*[**Operators to note this duty to report unauthorised access.]***

INTERNAL RISKS

Section 19: "Take appropriate reasonable, technical and organisational measures"		
Identify Internal risks	**List Controls**	**Review Effectiveness**
High volumes of personal information	Where is it stored: • Workpool system; • Dropbox; • Gmail; • VIP Payroll; • Xero; • Greatfsoft; • Pastel; • Adobe; • Lawactive; • CIPC	All these systems have privacy policies in place and protected passwords to log in.
Direct Marketing	Follow Policy steps	
Transfer of personal information to third parties	Written agreement	
Sending mail to wrong address or person	Triple check recipient and delete old email addresses	
Printing/filing	• Online; • Less printing • Printer behind closed doors; • Clients only allowed in Boardroom.	

EXTERNAL RISKS

Section 19: "Take appropriate reasonable, technical and organisational measures"		
Identify external risks	**List Controls**	**Review Effectiveness**
Break ins	Security gate, alarm system and secure windows	
hacking	• Encryption; • Anti-virus programs; • Passwords; • Screensavers	

SECURITY CHECKLIST

	OFFICE	**HOME**	**ACTION TO BE TAKEN**
PREMISES	**The Office** has security gate and secretary sitting at front door.	Safe Environment	Ensure that the office gate is permanently closed and no non-staff members allowed in office (only Boardroom)
FILING AND PHYSICAL RECORD KEEPING	Records kept in closets and less printing.		Lock up closets that contains any records
STAFF	Staff is aware of POPIA		Keep educating staff on the importance of POPIA
THIRD PARTY PROCESSING	Ensure that an agreement is put in place and that the data subject consents to third party processing		Set out clear terms of engagement
IT AND DATA	Security software		Update security software regularly
MOBILE DEVICES	Staff has a password on their mobile devices if it contains work related stuff.		
COMPUTERS	• Staff has a password on their computers and passwords on software programs; • Screensavers		
PAST SECURITY BREACHES	None		

WHAT HAPPENS IF THERE IS A SECURITY BREACH?

In terms of POPIA, **The office** and their operators cannot keep quiet and hope that no one will find out. The law puts an obligation on **The Office** and their operators to report the breach.

In terms of section 22: *Notification of security compromises.* —

(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised 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.

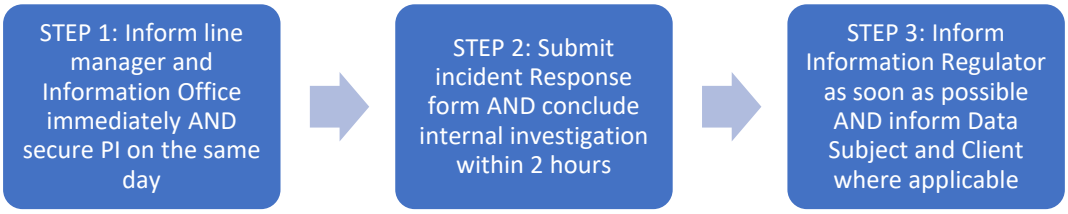
The law also determines that the notification to the data subject must be in writing and communicated in one of the following ways:

- mailed to the data subject's last known physical or postal address;
- sent by e-mail to the data subject's last known e-mail address;
- placed in a prominent position on the website of the responsible party;
- published in the news media; or
- as may be directed by the Regulator.

The following information needs to be disclosed in the notification:

- a description of the possible consequences of the security compromise;
- a description of the measures that the responsible party intends to take or has taken to address the security compromise;
- a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

BREACH OF STANDARD OPERATING PROCEDURES



Record	Description	Data subject	Responsible person	Retention period	Destruction method
Contract *(Standard terms of engagement)*	Hard copy and/or electronic file	Name of person whose information is included in the record	Employees	*As per Policy List (Data Retention Policy). Exception if exists*	Shred (if hard copy) Delete (if online)
Personal information	Hard copy and/or electronic file	Name of person whose information is included in the record	Employees	*As per Policy List (Data Retention Policy). Exception if exists*	Shred (hard copy) Delete (online)
Emails	Hard copy and/or electronic file	Name of person whose information is included in the record	Employees	*As per Policy List (Data Retention Policy). Exception if exists*	Shred (hard copy) Delete (online)
Record files	Hard copy	Name of person whose information is included in the record	Employees	*As per Policy List (Data Retention Policy). Exception if exists*	Shred
Record files	Electronic	Name of person whose information is included in the record	Employees	*As per Policy List (Data Retention Policy). Exception if exists*	Delete

CONCLUSION

The Office will consider applicable industry standards and make sure that they can comply with this important processing condition 7.

(Update Regularly)