Sensible Risk Solutions (Pty) Ltd

Company Registration No. 2014/204790/07 Vat No. 4330279342 FSP No. 48159

Sensible Risk Solutions

Physical Address
Wild Fig Business Park
1494 Cranberry Street
Block A, 1st Floor
Honeydew
2040

Postal Address
Suite 178
Private Bag X3
Strubens Valley
1735

Tel: +27 10 001 7590
www.sensiblerisk.com

Data Breach Response Plan

June 2024

This plan defines the steps to be taken in the event of loss of Personal Information, as a result of loss of, damage to, or unauthorised destruction of personal information, and unlawful access to or processing of personal information by an unauthorised entity.

The safekeeping of data whilst working remotely from home is an important consideration, to protect against access by unauthorised persons who might be able to view content on a laptop or cell phone.

A loss can arise from theft or loss of data storage media, such as computers or by cyber-attack. Experts deem the possibility of a cyber-attack to be a question of "when" and not "if" an incident occurs, thus the staff of Associated Compliance must be alert to the possibility of a breach and report any suspicion of a breach as soon as possible, to Craig Ormrod as the Information Officer (IO).

We must be aware of the possible risk of opening suspicious e-mails which might contain malicious links, which can lead to the installation of malware or a ransomware attack. It is felt that the threat of ransomware demand is probably a greater exposure than a cyber hack to steal information.

INCIDENT RESPONSE TEAM (IRT) Henry Ansara

Contact details:

Henry Ansara henry@sensiblerisk.com or 083 628 9901

BREACH DETECTION -

- Where there are reasonable grounds to believe that personal information has been accessed by an unauthorised person, or otherwise compromised, Craig Ormrod must be formally advised immediately by the person who identified the incident.
  The primary requirement is to identify the nature and extent of the incident and contain it, and to ensure the retention of all appropriate evidence. ***(Form DB1 – Data Breach Incident Report - to be completed by the person identifying the incident)***

- A written report of the circumstances relating to the incident must be completed ***(Form DB2 – Data Breach Assessment Report - to be completed by the Information Officer)***, once all relevant information has been obtained from the person who identified the event, in conjunction with IT Support and in association with IRT.

Sensible Risk Solutions (Pty) Ltd

Company Registration No. 2014/204790/07 Vat No. 4330279342 FSP No. 48159

Sensible Risk Solutions

Physical Address
Wild Fig Business Park
1494 Cranberry Street
Block A, 1st Floor
Honeydew
2040

Postal Address
Suite 178
Private Bag X3
Strubens Valley
1735

Tel: +27 10 001 7590
www.sensiblerisk.com

BREACH CONTAINMENT –

- Time and efficiency of response is a key factor in limiting any damage and IRT are to immediately take the necessary steps to secure the environment, contain the incident to prevent any further loss and to preserve any evidence. IRT will document information relating to the incident and perform an initial impact assessment.

NOTIFICATION REQUIREMENT -

Section 22 of the Protection of Personal Information Act (POPIA), (*Notification Security Compromises*), defines the steps required to notify the appropriate authorities in the event of a data breach.

- Notification must be given by Craig Ormrod as the Information Officer to the Information Regulator, ***(Form DB3 – Data Breach Notification form - to be completed by the Information Officer for this purpose)***. Data subject(s) must be advised once the Information Regulator has confirmed his/her satisfaction that the situation will not be compromised by notification to the data subject(s), and where appropriate, any Law Enforcement Agency should be notified, as soon as reasonably possible, again with the Information Regulator's approval.
- There are conditions applicable in this respect, primarily that notification to the data subject may be delayed if the Regulator or a Public Body, such as SAPS, determines that such notification will impede criminal investigation by any Public Body, or if it is perceived that notification of the breach to the data subject might cause an undesirable result, for example if the data relates to adverse health status, then the data subject's health practitioner or close relative, should be advised.
- The information given to the data subjects must provide sufficient information and be clear and specific, to enable them to understand the possible consequences of the security compromise. It must detail the measures we have taken in our attempt to avoid further compromise and unauthorised access or use of their personal information, and we must make recommendations to the data subjects as to how they can mitigate the possible adverse effects of the of the security compromise.
- Notification to the data subject must be in writing and communicated in at least one of the following ways:-
  1) Mail to the data subject's last known postal or physical address
  2) E-Mail to the data subject's last known e-mail address
  3) Prominent notification on our website (www.associatedcompliance.co.za)
  4) Published in the news or appropriate media, or

5) As may be directed by the Information Regulator

RECOVERY PROCESS –

- The procedures for the recovery from any incident will be identified once the containment processes have been completed. The means that the process for the recovery of data, if lost, will be confirmed, and activated by the IRT using any available assistance and advice. Decision will be made as to whether a phased approach to the reinstatement of systems will be a requirement or whether the entire system will be brought down and reinstated "in toto" once all issues have been resolved.

POST INCIDENT FOLLOW-UP–

- ***(Form DB4 – Data Incident/Breach Register - should be completed at this time by the Information Officer)***
- IRT will investigate, identify, and eradicate, where possible, any vulnerabilities which might become apparent during the investigation and handling of the incident.
- Interview anybody with insight relating to the occurrence and identify whether there were circumstances enabling the incident which could have been avoided, and install the necessary protections, including refresher training of staff, to prevent a recurrence.
- Ensure that data subjects (and our clients) have been fully informed as to the introduction of any procedures or steps taken which might affect their interaction with us after the incident.