POPIA - INCIDENT MANAGEMENT POLICY & PROCEDURE

of

WEALTH CREED (PTY) LTD

“FSP”

Table of Contents

Wealth Creed (Pty) Ltd | FSP 49447 | 010 312 6179 | info@wealthcreed.com
Adapt Executive Suites, 1st floor, 3 Gwen Lane, Sandton, 2196

1 Introduction

This is the official incident management policy of Wealth Creed to handle information security compromises in our organisation. As an authorised Financial Services Provider (FSP) and Accountable Institution (AI), the processing of personal information is central to our business. While we do our best to guard against information security incidents by having extensive policies in place, providing training from time to time and use technical tools to secure our information, security breaches still can and do occur. For this reason, it is imperative that we understand and are ready to apply this incident management policy.

2 Purpose

The purpose of this incident management policy is to set out the necessary procedures and protocols to address information security compromises or other related incidents in our organisation. This incident management policy is drafted with the aim of implementing good incident management practices to prevent or at least mitigate any harm that may be inflicted on us, our stakeholders, or the public in general.

3 Scope

This personal information management policy applies to all personal information held by the company relating to identifiable individuals, even if that information technically falls outside of the Protection of Information Act. This can include but not be limited to:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Remuneration;
- Race and Gender;
- Information external to the immediately knowledge of an employer;
- Any other information relating to individuals.

It is understood that personal information may also include sensitive personal information, and thus the compliance acknowledges the need for increased scrutiny of its safety, protection and security measures.

Wealth Creed (Pty) Ltd | FSP 49447 | 010 312 6179 | info@wealthcreed.com
Adapt Executive Suites, 1st floor, 3 Gwen Lane, Sandton, 2196

4 Roles and responsibilities

Top management:

Throughout the course of the protocol, top management is broadly responsible for:

- Ensuring that Wealth Creed meets its legal obligations;
- Ensuring that effective and efficient incident management procedures, protocols and training are in place.

Information officer:

Throughout the course of the protocol, the Information Officer is broadly responsible for:

- Coordinating efforts to manage an information security incident;
- Assembling a permanent or ad hoc security response team from relevant personnel from legal, human resources (HR), information technology (IT), any departments working with personal information and any external stakeholders where appropriate.
- Ensuring the prompt investigation of a security incident;
- Identifying what information may have been exposed;
- Securing any compromised systems to prevent further damage;
- Overseeing tasks performed by the security response team;
- Notifying the Information Regulator, relevant authorities, data subjects and any other affected stakeholders;
- Conducting post-incident analysis.

Security response team:

Throughout the course of the protocol, the security response team is broadly responsible for:

- Assisting the Information Officer with all delegated tasks and functions in response to the security breach.

5 Incident response phases

Incident Response Phases

The Incident Response process encompasses six phases including preparation, detection, containment, investigation, remediation and recovery. In the execution of responding to an incident, the Incident

Response Team will focus on the detection, containment, investigation, remediation and recovery of the specific incident.

Preparation

Preparation for incident response includes those activities that enable the organization to respond to an incident and include the creation and review of policies, standards and guidelines supporting incident response; security and technology related tools; effective communication plans and governance. Preparation also implies that the organizations across the university have implemented the controls necessary to enable the containment and investigation of an incident. As preparation happens outside the official incident process, process improvements from prior incidents should form the basis for continuous improvement at this stage.

Detection

Detection is the identification of an event or incident whether through automated means with security tools or notification by an inside or outside source about a suspected incident. This phase includes the declaration and initial classification of the incident.

Containment

Containment of an incident includes the identification of affected hosts or systems and their isolation or mitigation of the immediate threat. Communication with affected parties is established at this phase of incident response.

Investigation

Investigation is the phase where the security response team determine the priority, scope, risk and root cause of the incident.

Remediation

Remediation includes the repair of affected systems and services, addressing residual attack vectors against other systems, communication and instructions to affected parties and an analysis that confirms the threat has been contained.

Recovery

The recovery stage effectively requires a post-incident analysis that considers the possible procedural and policy implications. Further, recovery entails identifying ways in which security and incident management policy may be improved to deal with information security threats in the future.

6 Notification

The Information Officer is required in terms of POPIA to notify the Information Regulator, affected data subjects and supervisory authority, as the case may be, where there interference with the personal information of a data subject. Notification must take place 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 the Information Regulator and the data subject, unless the identity of such data subject cannot be established.

The notification must be made as soon as reasonably possible after the discovery of the breach, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the breach and to restore the integrity of the responsible party's information system. Where feasible notification should take place no later than seventy-two (72) hours after becoming aware of the information security breach.

The notification to a data subject must be in writing and communicated to the data subject in at least 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 directed by the Regulator.

The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Wealth Creed (Pty) Ltd | FSP 49447 | 010 312 6179 | info@wealthcreed.com
Adapt Executive Suites, 1st floor, 3 Gwen Lane, Sandton, 2196

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

- 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.

7. POPIA Incident Management Steps:

- All POPIA incidents must be recorded in the POPIA Incidents register on Kotive.
- Carefully follow the steps, populate the information accurately and upload all supporting information and records.

***STEP 1*: CONTAINMENT OF BREACH**

1. Attempt to recall the outlook email – this may allow us to delete the email from our side.
   How to recall an outlook email:
   1. *Select the Sent Items folder.*
   2. *Select or double-click the message so it opens in another window.*
   3. *Select File > Info.*
   4. *Select Message Resend and Recall > Recall This Message..., and select one of the two options. ...*
   5. *Select the Tell me if recall succeeds or fails for each recipient check box.*
   6. *Select OK.*
2. Send an email to the unintended recipient apologising for the incident and requesting that the unintended recipient delete the information (inbox and in sent folder).

3. Ask unintended recipient to sign an assurance letter wherein the unintended recipient warrants/ guarantees that the personal information has been deleted.

   - *If a person warrants/ guarantees a statement as being corrected that person agrees to be held contractually liable for the correctness of the statement.*
   - *This allows us to have recourse against someone if that person shares that information or uses that information later down the line.*
   - *The assurance letter will also assist us in providing the affected data subject with evidence of the measures taken to mitigate the damage.*

***STEP 2*: ASSESSMENT OF THE RISK**

1. Record a description of the breach/ circumstances of the breach of personal information in a report.
   1. *Record what personal information of the data subject was compromised, i.e. create a list of all the personal information that was compromised in the breach such as ID numbers, names, company registration number, account number etc.*
   2. *Record all the data subjects that could be affected by the breached;*
   3. *Describe how the data breach occurred;*
   4. *Record the identity of the unintended recipient.*

2. Compile an impact assessment report.

   1. *What is nature of the personal information (general personal information or sensitive personal information)?*
   2. *How many data subjects could be affected/ impacted by the data breach?*
   3. *What are the possible consequences of the data breach?*
   4. *What recommendations we can make to the data subject to mitigate any adverse consequences?*
   5. *What measures have been taken by us or do we intend to take to address the data breach?*

***STEP 3*: REPORT THE DATA BREACH**

1. Send a notification to all the affected data subjects.
   POPIA, section 22(5)

   The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

   a. *a description of the possible consequences of the security compromise;*

   b. *a description of the measures that the responsible party intends to take or has taken to address the security compromise;*

   c. *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*

   d. *if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.*

2. Send a letter apologizing to affected data subjects and ask if they are satisfied with the response taken or if there are any further measures that they feel we can take.

3. Send notification to information regulator (if applicable), i.e. if the severity of data breach justifies it or if data subjects are not happy with the response taken.

***STEP 4*: POST INCIDENT ANALYSIS**

1. Identify what steps can be taken to avoid breaches such as these reoccurring.

2. Identify how our response plan can be improved.