

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

TABLE OF CONTENTS

1. INTRODUCTION	2
2. PURPOSE	2
3. SCOPE	2
4. LEGISLATION	2
5. POLICY	2
6. RESPONSIBILITIES AND AUTHORITY	2
7. IDENTIFICATION OF INCIDENTS	3
7.1. INCIDENTS	3
7.2. CATEGORIES	3
8. REPORTING OF INCIDENTS	4
8.1. ACCOUNTABILITY	5
8.2. DETAIL	5
8.3. AUTHORITIES	5
8.4. REQUESTS TO COOPERATE	5
8.5. PROTECTION	5
8.6. OPTIMAL ANONYMITY	5
9. RESPONSE TO INCIDENTS	6
9.1. RESPONSE TEAM	6
9.2. CONTAINMENT AND RECOVERY	6
9.3. NOTIFICATION	6
9.4. NOTIFICATION TIMEFRAME	7
9.5. NOTIFYING AUTHORITIES	7
9.6. NOTIFYING DATA SUBJECTS	7
9.7. NOTIFICATION QUESTIONS	8
9.8. MANNER	8
9.9. ACKNOWLEDGEMENT	8
9.10. APOLOGY	9
9.11. COMMUNICATE	9
10. EVALUATION OF OUTCOME OF RESPONSE	9
10.1. QUESTIONS	10
10.2. POLICY UPDATE	10
10.3. INFORMATION SECURITY UPDATE	10
11. AUTHORISATION AND APPROVAL	10

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

Confidential

For Internal use only

Page 1 of 11

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

1. INTRODUCTION

The Incident Response Policy for the De Beers Pension Fund ("the Fund") sets out the official Policy that the Fund will follow should there be any breach to the private and confidential information held by the Fund. Information is a powerful tool that the Fund relies on to conduct its business.

Should there be a data breach of confidential and/or personal information, the Fund faces significant risks if such data falls into the wrong hands. The Fund has invested significant resources to ensure that it does its best to guard against potential incidents and breaches, to have appropriate policies in place, provide training from time-to-time, and use technical tools to secure and protect its confidential and personal information where appropriate.

Despite the preventative measures implemented, this Incident Response Policy is to be used as an aid to understand and be ready to respond to any breach or potential breach of confidential or personal information held by the Fund.

2. PURPOSE

The purpose of this Policy is to set out the necessary steps to effectively and efficiently identify, report, escalate, respond to, and evaluate whether the Fund has resolved any data/personal information security compromises or other related incidents that may occur in the Fund. It is important as the Fund needs to implement industry best practices to deal with incidents that may harm it, or any of its stakeholders.

3. SCOPE

This Policy is applicable to the Fund.

4. LEGISLATION

This Policy gives effect to many of the responsibilities that the Fund carries out in terms of the processing and storage of personal information and as contained in the Protection of Personal Information Act 4 of 2013 (**POPIA**) and should be read in conjunction with that Act where applicable.

5. POLICY

The objective of this Policy is to guide the official response for handling information security breaches in respect of confidential and/or personal information held by the Fund.

6. RESPONSIBILITIES AND AUTHORITY

This Policy is the responsibility of the Fund's Information Officer or anyone delegated with the responsibility of responding to security breaches and related incidents faced by the Fund. The Principal Officer, in consultation with the Information Officer and the Chairman of the Board, is the only person in the Fund that is authorised to speak on behalf of the Fund about information security breaches or other related incidents. The Information Officer is responsible for responding to security breaches. This means that all incidents (real or potential) must be reported to the Information Officer who must:

- Inform the Principal Officer /Board of Trustees of any breach/potential breach;

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

- Authorise all notifications to the Regulator, the authorities, or data subjects in writing in consultation with the Principal Officer;
- Approve all external communications about an incident in consultation with the Principal Officer;
- Decide where and how to allocate resources to handle incidents;
- Assemble a response team and instruct them on their specific responsibilities; and
- Manage the response team on an ongoing basis until the incident has been successfully resolved.

7. IDENTIFICATION OF INCIDENTS

Once it has been ascertained and confirmed that the Fund has suffered a breach of its confidential and/or personal information, the Information Officer must investigate and understand the exact nature and extent of the breach to determine the appropriate course of action and the response required.

7.1. INCIDENTS

An incident is a security breach or any other related incident where there are reasonable grounds to believe that the personal information belonging to the Fund's members and/or other stakeholders has been accessed or acquired by any unauthorised person.

This definition has three components:

- **Reasonable grounds to believe** – an average person would reasonably accept that there was a security breach from the circumstances and available confirmed information;
- **Personal information of a data subject** – the security breach compromises personal information belonging to a data subject (such as members for example); and
- **Accessed or acquired by any unauthorised person** – someone who is not permitted or entitled to have accessed or acquired the personal information has done so.

Incidents will include (but not limited to) anything that meets the following criteria:

- **Loss or theft** of data containing personal information or equipment on which data containing personal information is stored;
- **Hacking** or any other deliberate attack on the Fund's computer systems to access data containing personal information;
- **Access control failure** – a failure of a password, firewall, or other access control system that allowed unauthorised access to personal information;
- **Unauthorised use** of personal information by a member of the Fund staff;
- **Equipment failure** – failed equipment that exposes personal information to unauthorised access;
- **Human error** – a person making a mistake that exposes personal information to unauthorised access; or
- **Phishing** or other ways of using persuasion or guile to obtain personal information without authorisation.

7.2. CATEGORIES

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

Once an incident has been identified, it must be categorised. A category is a class of incidents based on shared characteristics. This Policy does not prescribe hard and fast categories into which incidents should be categorised, it merely suggests a few ways of categorising them – for example, an incident could be categorised based on:

- The **sensitivity** of any confidential or personal information leaked during the incident – e.g. is it less sensitive information that may be publicly available elsewhere, information of a personal nature vulnerable to misuse, or highly sensitive information like a member's personal medical history, the wrongful disclosure of which is an offence under POPIA;
- How badly the incident threatens the Fund's **reputation** – e.g. is it a small transgression that can easily be handled or is it an incident that could significantly threaten the reputation of Fund irreversibly;
- How difficult the incident will be to **recover** from – e.g. is it a simple matter of distributing a well written response or is it a larger problem that may need a series of responses;
- The **severity** of the incident and the consequences to the data subjects involved in the incident – e.g. will it merely inconvenience members, or does it entail long-term and far reaching potential adverse consequences for members;
- What **type** of personal information is involved – e.g. is it easily accessible personal information, special personal information that requires additional protection, or a special class of personal information such as account numbers, special personal information such as medical history or salary information, or the personal information of children;
- How **protected** is the stolen personal information – e.g. if it was stored on stolen equipment and was that equipment and/or were the relevant files encrypted;
- What has **happened** to the personal information – e.g. the risk will result in potential harm to data subjects if equipment has been stolen and the personal information is accessible to the party who has stolen the equipment, or the risk may only be the loss of personal information if equipment has been damaged but is still in the Fund's possession;
- **Who** has accessed or acquired the personal information without authorisation – e.g. an opportunistic thief stealing a laptop may have little interest in the personal information stored on the device, while a determined fraudster may use personal information gleaned from phishing to cause significant harm;
- What is the **extent** of the security breach or related incident – e.g. how many data subjects had their personal information accessed or acquired without authorisation;
- Who are the **data subjects** whose personal information has been breached – e.g. were they members, employees, contractors, or service providers to the Fund; and
- What **harm** could come to those data subjects – e.g. what are the risks to their safety, reputation, finances, or other aspects of their lives or businesses?

8. REPORTING OF INCIDENTS

The Information Officer must complete a written report of the incident in order to deal with the incident correctly and in terms of this Policy by completing the Incident Reporting Form (Annexure A). All staff are encouraged to report an incident or any suspected incident and to provide as much detail as possible to the Information Officer to allow the completion of

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

the Incident Reporting Form. The contact details of the Information Officer should be easily accessible to all Fund staff should they wish to report an incident.

8.1. ACCOUNTABILITY

The Fund must encourage staff, members, website administrators and system related service providers to bring any suspected incidents to the Information Officer's attention as quickly as possible. They must report any incident directly to the Information Officer so that the incident can be managed in accordance with this Policy. Any delays in reporting an incident can determine how effectively the Fund is able to manage the incident.

8.2. DETAIL

It is important that the Fund has any incident reported within two working days in sufficient detail to enable the Information Officer to process and manage it effectively. Anyone reporting an incident should provide all the possible information available and will also be required to complete the Incident Reporting Form (Annexure A).

8.3. AUTHORITIES

Only the Information Officer in consultation with the Principal Officer should decide whether to contact the Regulator, law enforcement, or other authorities about a particular incident. Despite the best intentions, reporting an incident to the authorities could seriously disrupt the business. The authorities could seize Fund equipment for evidential reasons which could prevent staff members from performing their duties. The decision to report an incident to the authorities should therefore be left to the Information Officer in consultation with the Principal Officer who will consider it carefully before doing so.

8.4. REQUESTS TO COOPERATE

Fund staff or system service providers should be cautioned not to reply to any requests to cooperate with any investigations about incidents unless the requests come directly from the Fund's Information Officer. Hackers can use phishing techniques combined with the uncertainty of how to deal with an incident to obtain sensitive information from staff or service providers. These requests may appear to come from the Regulator, law enforcement, staff or other authorities – but these requests must be submitted to the Fund's Information Officer who will decide whether they are legitimate or not.

8.5. PROTECTION

The Fund encourages staff and service providers to report incidents and will not disclose their identity to make sure that they are comfortable reporting any potential incidents. If an employee or service provider reports an incident in good faith (which means that they did not intentionally cause the incident themselves or help someone else cause it), then they should not be threatened with any claims or consequences because of their involvement in the incident. There should be no recourse against those that report incidents even if it is established that there was no incident or that the incident did not pose any risk.

8.6. OPTIMAL ANONYMITY

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

Confidential

For Internal use only

Page 5 of 11

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

If a Fund staff member or a service provider reports an incident, they may tell the Information Officer whether or not they wish to remain anonymous. If they elect to remain anonymous, then the Information Officer will not provide their identifying information to anyone else unless absolutely necessary (for example, as required by law enforcement to proceed with their case).

9. RESPONSE TO INCIDENTS

The Fund must respond appropriately to an incident, which is crucial in managing any breach effectively. The cost of an incident is often determined by how well it is responded to upfront.

9.1. RESPONSE TEAM

The Information Officer should assemble and oversee a response team consisting of representatives from business areas and external service providers likely to be involved in dealing with a security breach or any other related incident and should consider including representatives from:

- Legal advisors;
- Human resource consultants (HR);
- Information technology (IT);
- Any other departments working with personal information; and
- Certain external stakeholders such as system service providers where appropriate.

The Information Officer needs to decide whether to delegate responsibility to members of the response team. The Information Officer must clearly document and define the roles of the response team. Each person should be responsible for different tasks, and they should understand that the Information Officer oversees them. The Information Officer should have a clear plan of communication within the team.

9.2. CONTAINMENT AND RECOVERY

Any response to a security breach, data breach or related incident should be backed up by a containment and recovery plan that seeks to limit the damage caused by the incident. The plan should specify which member of the response team will lead the containment and recovery process and must establish the roles and responsibilities of each team member.

9.3. NOTIFICATION

The Information Officer needs to know who to notify in the case of a security breach, whether it be the Regulator, data subjects (such as members), and law enforcement authorities. There are legal requirements in terms of POPIA to notify certain parties about security breaches and related incidents that must be adhered to when responding to an incident. However, there are also business reasons why the Fund should notify certain parties including the Chairperson of the Audit and Risk Board Committee. The Information Officer, in consultation with the Principal Officer, will decide whether to notify third parties about a security breach or related incident.

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

9.4. NOTIFICATION TIMEFRAME

Section 22(2) of POPIA requires the Fund to make a notification as soon as possible after an incident is discovered because:

- Law enforcement authorities need time to respond;
- Reasonable measures need to be taken to determine the scope of the breach; and
- The integrity of the information system needs to be restored.

However, the Information Officer must ensure that he/she does not breach the steps set out in this Policy by making a notification prematurely.

9.5. NOTIFYING AUTHORITIES

Section 22(1)(a) of POPIA requires the Fund to notify the Information Regulator of a data breach that compromises data subjects personal and/or confidential information. The purpose of the notification is to allow the appropriate regulatory bodies to perform their functions. It is important that the Fund notifies the correct regulatory body. When notifying the regulatory body, details should be provided about what the Fund is prepared to do to help the Regulator. Consideration must be given to notifying other third parties such as law enforcement bodies, insurers, professional bodies, bank or credit card companies, trade unions, and anyone else who may be able to assist in reducing the risk of financial loss to members and/or the Fund. The Regulator may direct the Fund in terms of section 22(6) of POPIA to publicise the fact that the integrity or confidentiality of its personal information has been breached if they believe that the publicity would protect an affected data subject. It is important that the Regulator is only notified where there is a real and serious security breach or related incident.

9.6. NOTIFYING DATA SUBJECTS

Section 22(1)(b) of POPIA requires the Fund to notify the data subjects affected by the incident unless their identity cannot be established. The Fund may only delay notifying the data subjects in terms of section 22(3) of POPIA if a public body responsible for the prevention, detection, or investigation of offences or the Regulator determines that notification will impede their criminal investigation. Section 22(4) of POPIA requires the notification to the data subject to be in writing and communicated in at least one of the following ways:

- Physically delivered to the data subject's last known physical or postal address;
- Electronically delivered to the data subject's last known e-mail address;
- Placed in a prominent place on the Fund's website;
- Published in the news media; or
- As the Regulator may direct.

Section 22(5) of POPIA requires the notification to the data subject to contain enough information to allow the data subject to take steps against the consequences of the breach, including:

- A description of the possible consequences of the incident;
- A description of the steps that the Fund intends to take to handle the security breach;
- Suggestions of what the data subject could do to mitigate the consequences of the security breach; and
- The identity of the unauthorised person/entity (if established and confirmed).

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

9.7. NOTIFICATION QUESTIONS

In order to establish if data subjects need to be notified of a security breach, the Information Officer can use the following questions as an aid to determine whether notification is required:

- Is the Fund legally or contractually obliged to notify anyone about the incident – i.e. are there legal obligations to notify the Regulator and the data subjects?
- Will the notification help the individual data subject – i.e. bearing in mind the potential effects of the breach, would data subjects be able to act on the information provided to mitigate their risks?
- What is the Fund required to communicate to make the notification appropriate for a particular group of data subjects – for example, is the communication directed at children or adults?
- What are the risks of **not** notifying the data subject? – i.e. will the data subject lose trust in the Fund or try to sue the Fund if they become aware of the non-notification?
- What are the risks of 'over notifying' – i.e. not every incident requires notification of all data subjects and only the affected subset of data subjects may need be notified.

9.8. MANNER

It is important that the Fund frame and deliver its communication in response to a security breach in the correct manner, which includes:

- Keeping the response **simple** – complexity means more room to make mistakes;
- Delivering the response **quickly** – failing to respond quickly makes the problem worse and provides data subjects who were affected more time to control the message, and makes the general public believe that the Fund are uninterested in the security breach;
- Delivering the response as a matter of **urgency** where the fallout is severe – the first 24 hours are crucial, the internet/social media will not wait for a Fund response and news will spread with or without the Fund's involvement;
- Making sure that the Fund has a well thought out response and responding properly means going to the source of the complaints and interacting with the relevant audience;
- Delivering the response in an **appropriate forum** – take any negative conversations private as soon as possible to reduce the chance of them causing harm; and
- Not admitting **liability** – but still being sympathetic about bad experiences.

The Fund will have successfully responded to an incident if:

- The Fund leadership is accountable;
- The Fund is able to re-establish trust; and
- The incident is responded to and managed in a transparent manner.

9.9. ACKNOWLEDGEMENT

To determine the seriousness of a security breach or other related incident, the following information must be collected:

- Who or what was affected by the incident;
- Why did the incident occur;
- When and where did the incident occur;

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

- How did the incident occur;
- To what extent did the incident pose a risk;
- Who was responsible for the incident;
- What data was breached;
- Which data subjects are affected by the breach; and
- How did we find out about the incident?

While the Fund should collect all the above information, it should also decide whether or not it wishes to communicate all the information to the affected data subjects. Certain information must be communicated to affected data subjects by law, but beyond that – the Information Officer, in consultation with the Principal Officer, should decide on what additional information should be communicated.

9.10. APOLOGY

The Fund needs to apologise for a security breach or other related incident, which means acknowledging it sympathetically. An incident may cause data subjects a number of negative feelings, including anxiety, inconvenience, and doubt. It is the Fund's duty to address these emotions by acknowledging them. This reassures the data subject that the Fund cares about the emotional or other potential fallout of the incident, which will help resolve it. The apology should contain an acknowledgement that the Fund is listening to data subjects, seeking answers as to why the incident occurred, what action has been taken to date and any further actions planned in the future and that the Fund is genuinely sorry. Such a statement contributes towards a feeling of forgiveness as well as to quell anger and resentment. However, the apology should not amount to admitting liability. The Information Officer should have a legal representative on the response team for this reason. It is very important that the apology does not focus on management or the organisation. Make the apology about the data subject – they are the ones that matter.

9.11. COMMUNICATE

The Fund needs to communicate to data subjects what has already been done to manage the data breach. This involves using all forms of media (including the Fund's website and emails) to its advantage to increase the reach of the response. It is made up of three distinct tactics:

- The Fund needs to **amplify** the response by directing members to the right information about the incident on the Fund's website;
- The Fund needs to find **advocates/supporters** to help spread the appropriate response in the form of HR managers at each of the working member sites/operations who can be galvanised to carry the message; and
- The Fund needs **adhesion**, which involves adhering to its corporate image and values, being clear about what it will and will not do and adhering to this Policy.

10. EVALUATION OF OUTCOME OF RESPONSE

A security breach or other related incident is not over once the Fund has responded to it. The outcome to that response needs to be evaluated with a retrospect being performed by the Information Officer as to whether any additional or follow-up communication is needed or whether the response that was initially distributed was sufficient.

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

10.1. QUESTIONS

Security breaches or other related incidents can be confusing to deal with and this Policy cannot cover all issues associated with these incidents. There may be issues/incidents that fall outside of this Policy. Any Board or staff member should contact the Information Officer with questions when such incidents occur or if they have any Policy-related questions.

10.2. POLICY UPDATE

This Policy must be reviewed annually and amended based on learnings should an incident have happened during the period under review.

10.3. INFORMATION SECURITY UPDATE

The Fund must update its information security systems based on the outcome of the incident and the response. Information security is a constantly changing landscape. Section 19(3) of POPIA requires the Fund to have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of industry rules and regulations.

11. APPROVAL

Approved by the Board of Trustees.



CHAIRPERSON OF THE FUND

C J Blanckenberg

Date: 16/5/2019

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

Confidential

For Internal use only

Page 10 of 11

POLICY					
Owner	De Beers Pension Fund				
Subject	Incident Response Policy				
Revision no	0	Review cycle	Yearly	Effective date	27 March 2019

REVISION HISTORY

Revision no	Date reviewed	Date approved	Minute No.
000	Policy drafted and approved	27 March 2019	5.19.7

UNCONTROLLED COPY

This copy is only valid for 24 hours after printed date (16 May 2019)

Confidential

For Internal use only

Page 11 of 11



ANNEXURE A

**DE BEERS PENSION FUND
INTERNAL INCIDENT REPORTING FORM
FOR THE ATTENTION OF THE INFORMATION OFFICER**

Date and time of incident	
Name of person reporting the incident	
Contact details of the person reporting the incident	
Cell number:	Email:
Describe fully what occurred re this incident	
Who or what was and/or could be affected by the incident?	
Where and when did the incident occur?	
Why did the incident occur?	
How did you find out about the incident?	

Signature:_____ **Date:**_____

Information Officer to complete the following:

How did the incident occur?
To what extent does the incident pose a risk? / Should a communication be directed towards the affected data subjects (members)?
Who was responsible for the incident?
What data/information was compromised by the incident?
Which members/stakeholders are potentially affected by the incident?
Was the incident as a result of negligence by a third-party contractor and is there liability associated in terms of the contract?
Are there any other stakeholders that must be notified of the incident?
If communication is required to the stakeholders / data subjects - what format should the communication take (email, website letters)?
Is the DBPF legally or contractually obliged to notify anyone about the incident – i.e. are there legal obligations to notify the Regulator and the data subjects?

Signature:_____ **Date:**_____