

DE BEERS BENEFIT SOCIETY

SOCIETY POLICY DOCUMENT

INCIDENT RESPONSE POLICY

<u>Revision no</u>	<u>Review cycle</u>	<u>Effective date</u>
1	At least every two years	25 March 2020



A registered medical scheme
Registration no. 29/4/2/1068

Society Policy Document					
Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

TABLE OF CONTENTS

1. PURPOSE	3
2. SCOPE.....	3
3. DEFINITIONS AND ACRONYMS	3
4. RESPONSIBILITIES AND AUTHORITY	3
5. POLICY	3
5.1 IDENTIFICATION OF INCIDENTS	3
5.2 INCIDENTS.....	4
5.3 CATEGORIES	4
5.4 REPORTING OF INCIDENTS.....	5
5.5 ACCOUNTABILITY	5
5.6 DETAIL	5
5.7 AUTHORITIES.....	6
5.8 REQUESTS TO COOPERATE.....	6
5.9 PROTECTION.....	6
5.10 OPTIMAL ANONYMITY	6
5.11 RESPONSE TO INCIDENTS.....	6
5.12 RESPONSE TEAM	6
5.13 CONTAINMENT AND RECOVERY	7
5.14 NOTIFICATION.....	7
5.15 NOTIFICATION TIMEFRAME.....	7
5.16 NOTIFYING AUTHORITIES	7
5.17 NOTIFYING DATA SUBJECTS.....	8
5.18 NOTIFICATION QUESTIONS.....	8
5.19 MANNER	9
5.20 ACKNOWLEDGEMENT	9
5.21 APOLOGY	9
5.22 COMMUNICATE	10
5.23 EVALUATION OF OUTCOME OF RESPONSE	10
5.24 QUESTIONS.....	10
5.25 INFORMATION SECURITY UPDATE	10
6. AUTHORISATION AND APPROVAL	11
ANNEXURE A – INCIDENT REPORTING FORM	12
REVISION HISTORY	14

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

1. 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 Society has resolved any personal/confidential information/data (hereinafter referred to as personal information) security compromises or other related incidents that may occur in the Society. It is important as the Society needs to implement industry best practices to deal with incidents that may harm it, or any of its stakeholders.

2. SCOPE

This Policy is applicable to the Society.

3. DEFINITIONS AND ACRONYMS

Definition/Acronym	Description
POPIA	The Protection of Personal Information Act No. 4 of 2013

4. RESPONSIBILITIES AND AUTHORITY

This Policy is the responsibility of the Society Information Officer, or anyone delegated with the responsibility of responding to security breaches and related incidents faced by the Society.

The Principal Officer, in consultation with the Society Information Officer and the Chairperson of the Board, is the only person in the Society that is authorised to speak on behalf of the Society 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 Society Information Officer who in turn must:

- inform the Principal Officer of any breach/potential breach;
- authorise all notifications to the Information 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; and
- draft a response plan with specific responsibilities and timelines in order to:
 - 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.

5. POLICY

5.1 IDENTIFICATION OF INCIDENTS

Once it has been ascertained and confirmed that the Society has suffered a breach of its members' or other stakeholders' personal information, the Society Information Officer must investigate and understand the exact nature of the breach to determine the appropriate course of action and the response required.

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

5.2 INCIDENTS

An incident is a security compromise or any other related incident where there are reasonable grounds to believe that the personal information of Society 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 compromise 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 anything that meets these criteria, which could include:

- **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 Society'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 Society's 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.

5.3 CATEGORIES

Once an incident has been identified, it must be categorised. A category is a class of incident(s) 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 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 medical history, or diseases that a member may have, the wrongful disclosure of which is an offence under POPIA;
- how badly the incident threatens the Society's **reputation** – e.g. is it a small transgression that can easily be handled or is it an incident that could significantly threaten the Society 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 large problem that needs a series of responses;

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

- the **severity** of the incident and the consequences to the data subjects (such as members) involved in the incident – e.g. will it merely inconvenience them, or does it entail long-term and far reaching potential adverse consequences for them;
- 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 equipment that was stolen, was that equipment and/or 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 Society'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 compromise 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 compromised – e.g. were they members, employees, contractors, or service providers to the Society; 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?

5.4 REPORTING OF INCIDENTS

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

5.5 ACCOUNTABILITY

The Society must encourage staff, members, website administrators and system related service providers to bring any suspected incidents to the Society Information Officer's attention as quickly as possible. They must report any incident directly to the Society 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 Society is able to manage the incident.

5.6 DETAIL

It is important that the Society has any incident reported in sufficient detail to enable the Society 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).

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

5.7 AUTHORITIES

Only the Society Information Officer in consultation with the Principal Officer should decide whether to contact the Information 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 Society equipment for evidential reasons which could prevent Society staff members from performing their duties. The decision to report an incident to the authorities should therefore be left to the Society Information Officer in consultation with the Principal Officer who will consider it carefully before doing so.

5.8 REQUESTS TO COOPERATE

Society 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 Society Information Officer. Hackers can use phishing techniques combined with the uncertainty of how to deal with an incident to obtain personal information from staff or service providers. These requests may appear to come from the Information Regulator, law enforcement, or other authorities, but it is best to send these requests to the Society Information Officer who will decide whether they are legitimate or not.

5.9 PROTECTION

The Society 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 a Society staff member 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 recourse or discrimination against them in any way 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.

5.10 OPTIMAL ANONYMITY

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

5.11 RESPONSE TO INCIDENTS

The Society 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.

5.12 RESPONSE TEAM

The Society 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 compromise or any other related incident and should consider including representatives from:

- legal;
- human resources (HR);

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

- information technology (IT);
- any other departments working with personal information; and
- certain external stakeholders such as system service providers where appropriate. The Society Information Officer needs to decide whether to delegate responsibility to members of the response team. The Society 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 Society Information Officer oversees them. The Society Information Officer should have a clear plan of communication within the team.

5.13 CONTAINMENT AND RECOVERY

Any response to a security compromise, 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 establish the roles and responsibilities of each team member.

5.14 NOTIFICATION

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

5.15 NOTIFICATION TIMEFRAME

Section 22(2) of POPIA requires the Society to make a notification (where applicable) 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 compromise; and
- the integrity of the information system needs to be restored.

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

5.16 NOTIFYING AUTHORITIES

Section 22(1)(a) of POPIA requires the Society to notify the Information Regulator of a data breach that compromises data subjects' personal information.

The purpose of the notification is to allow the appropriate regulatory bodies to perform their functions. It is important that the Society notifies the correct regulatory body. When notifying the regulatory body, details should be provided about what the Society is prepared to do to help the Information 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 Society.

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

The Information Regulator may direct the Society in terms of section 22(6) of POPIA to publicise the fact that the integrity or confidentiality of its personal information has been compromised if they believe that the publicity would protect an affected data subject. It is important that the Information Regulator is only notified where there is a real and serious security compromise or related incident.

5.17 NOTIFYING DATA SUBJECTS

Section 22(1)(b) of POPIA requires the Society to notify the data subjects affected by the incident unless their identity cannot be established by the compromised data. The Society 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 Information 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;
- electronically delivered to the data subject last known cell number by SMS;
- placed in a prominent place on the Society website;
- published in the news media; or
- as the Information 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 compromise, including:

- a description of the possible consequences of the incident;
- a description of the steps that the Society intends to take to handle the security compromise;
- suggestions of what the data subject could do to mitigate the consequences of the security compromise; and
- the identity of the unauthorised person/entity (if established and confirmed).

5.18 NOTIFICATION QUESTIONS

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

- is the Society legally or contractually obliged to notify anyone about the incident – e.g. are there are legal obligations to notify the Information Regulator and the data subjects?
- will the notification help the individual data subject – e.g. 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 Society required to communicate to make the notification appropriate for a particular group of data subjects – e.g. is the communication directed at children or adults?
- what are the risks of not notifying the data subject? – e.g. will the data subject lose trust in the Society or try to sue the Society if they become aware of the non-notification?
- what are the risks of 'over notifying' – e.g. not every incident requires notification of all data subjects and only the affected subset of data subjects may need be notified?

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

5.19 MANNER

It is important that the Society frame and deliver its response 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 upset more time to control the message, and makes the public believe that the Society 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 Society response and news will spread with or without the Society's involvement;
- making sure that the Society has a well thought out response and responding properly means going to the source of the complaints and interacting with the audience there;
- 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 Society will have successfully responded to an incident if:

- the Society leadership is accountable;
- the Society can re-establish trust; and
- the incident is responded to and managed in a transparent manner.

5.20 ACKNOWLEDGEMENT

To determine the seriousness of a security compromise 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;
- how did the incident occur;
- to what extent did the incident pose a risk;
- who was responsible for the incident;
- what data was compromised;
- which data subjects are affected by the compromise; and
- how did we find out about the incident?

While the Society 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 Society Information Officer, in consultation with the Principal Officer should decide on what additional information to communicate.

5.21 APOLOGY

The Society needs to apologise for a security compromise or other related incident, which means acknowledging it sympathetically. An incident may cause data subjects a number of negative

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

feelings, including anxiety, inconvenience, and doubt. It is the Society's duty to address these emotions by acknowledging them. This reassures the data subject that the Society cares about the emotional or other potential fallout of the incident, which will help resolve it.

The apology should contain an acknowledgement that the Society 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 Society 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 Society 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.

5.22 COMMUNICATE

The Society 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 Society's website, email and SMS services) to its advantage to increase the reach of the response. It is made up of three distinct tactics:

- The Society needs to amplify the response by directing data subjects (such as members) to the right information about the incident on the Society's website;
- The Society 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 Society needs adhesion, which involves sticking to its corporate image and values, being clear about what it will and will not do and sticking to this Policy.

5.23 EVALUATION OF OUTCOME OF RESPONSE

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

5.24 QUESTIONS

Security compromises or other related incidents can be confusing to deal with, but this Policy cannot cover all issues when it comes to security compromises or other related incidents. There may be issues/incidents that fall outside of this Policy. Any Board or Board Committee member or staff member should contact the Society Information Officer with questions when such incidents occur or if they have any questions arising out of this Policy.

5.25 INFORMATION SECURITY UPDATE

The Society 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 Society 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.

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

6. AUTHORISATION AND APPROVAL

Approved by the Board of Trustees.



CHAIRPERSON OF THE SOCIETY
C J Blanckenberg

Date: 26/3/2020

Society Policy Document					
Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

ANNEXURE A – INCIDENT REPORTING FORM

DE BEERS BENEFIT SOCIETY

INTERNAL INCIDENT REPORTING FORM

FOR THE ATTENTION OF THE SOCIETY 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 affected by the incident?	
When and where did the incident occur?	
Why did the incident occur?	
How did you find out about the incident?	

Society Policy Document

Organisation	De Beers Benefit Society (the Society)				
Subject	Incident Response Policy				
Revision no	001	Review cycle	At least every two years	Effective date	25 March 2020

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 (such as members)?
Who was responsible for the incident?
What data/information was compromised by the incident?
Which members/stakeholders are 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, etc.)?
Is the Society legally or contractually obliged to notify anyone about the incident – e.g. are there are legal obligations to notify the Information Regulator and the data subjects?
Is there a loss to the Society? Notify Insurers?

Society Policy Document

Organisation	De Beers Benefit Society (the Society)			
Subject	Incident Response Policy			
Revision no	001	Review cycle	At least every two years	Effective date 25 March 2020

REVISION HISTORY

Revision no	Description	Date Reviewed	Date Approved	Minute no
000	Policy drafted and approved	March 2019	27 March 2019	5.19.7
001	Reviewed	March 2020	25 March 2020	11.20.3