GoMobile (Pty) Ltd

Incident Response Policy

March 2021 | Version 1.0

1. Introduction

This is our official incident response policy to handle information security compromises in our organisation. Information is a powerful tool that we rely on to run our business. But, it poses significant risks if it falls into the wrong hands because of a security compromise or related incident that lets an unauthorised person access or acquire any personal information contained in it.

We do our best to guard against incidents and have policies in place, provide training from time to time, and use technical tools to secure our information.

But, incidents still can and do occur. For this reason, we must understand and be ready to apply this incident response policy.

2. Purpose

This document is internally focused.
The purpose of this policy is to set out the necessary steps to effectively and efficiently identify, report, escalate, respond to, and evaluate whether we have resolved any security compromises or other related incidents that occur in our organisation.

It is important because we must implement good incident management practices to deal with incidents that may harm us, our stakeholders, or the public in general.

This policy sets out the process for handling a security compromise or any other related incident.

3. Legislation

This policy gives effect to our responsibilities as a responsible party or operator in terms of the Protection of Personal Information Act 4 of 2013 (**POPIA**) and as a controller or processor in terms of the General Data Protection Regulation 2016/679 (**GDPR**) and should be read in conjunction with that legislation where applicable.

This policy should be read in conjunction with POPIA and GDPR.

4. Audience

This policy is intended primarily for our Information Officer (IO) and anyone tasked to assist in responding to security compromises and related incidents by the IO. This policy is important for our IO, or someone that they have delegated appropriate authority to, because it could affect how they handle a security compromise or other related incident.

They are also the only people in our organisation that should be authorised to speak on our behalf about security compromises or other related incidents.

The IO is responsible for responding to security compromises. This means that:

- In general, all incidents must be reported to the IO [or the office of the IO];
- The IO must authorise all notifications to the Regulator, the authorities, or data subjects in writing, although they need not make them themselves;
- The IO must approve all external communications about an incident;
- The IO must decide where and how to allocate resources to handle incidents; and
- The IO must assemble a response team and instruct them on their specific responsibilities.

5. Report

We must have information of the incident so that we can deal with it properly. If we don’t know about it, then we can’t do anything about it.

We want anyone at any level of our organisation to be encouraged to report an incident to us.

We also want them to report incidents in sufficient detail for us to formulate a meaningful response. The contact details of the IO should be easily accessible when anyone wants to report an incident.

Have the incident reported.

5.1. ***Duty***. We must encourage employees, partners and contractors (and even our customers and prospects where appropriate) to bring any suspected incidents to our attention as quickly as possible.

They must report them directly to our IO so that we can handle them properly. It is very important that we encourage the reporting of all incidents as soon as humanly possible, because it is often required by law and delays in finding out about incidents can determine how effectively we are able to manage them.

We must encourage employees, partners and contractors to bring any suspected incidents to our attention by reporting them to our IO as quickly as possible.

5.2. ***Detail***. It is important that we have any incident reported in sufficient detail to enable the IO to process it effectively.

Anyone reporting an incident should provide the IO with all possible information. It is better for them to give the IO too much information than for them not to give the IO enough information.

Employees or contractors should report incidents in sufficient detail to the IO.

5.3. ***Authorities***. Only the IO should decide whether or not to contact the Regulator, law enforcement, or other authorities about a particular incident as they are in charge of the incident response procedure.

Despite the best intentions, reporting an incident to the authorities could seriously disrupt our business. The authorities could seize our equipment for evidential reasons which could prevent our employees or contractors from doing their everyday work.

The decision to report an incident to the authorities should therefore be left to the IO (or anyone the IO has delegated the responsibility to) who will consider it carefully before doing so.

Only the IO should decide if, when, and how to report an incident to the Regulator, law enforcement, or other authorities, not our employees or contractors themselves.

5.4. ***Requests to cooperate***. Our employees, partners or contractors should be cautioned not to reply to any requests to cooperate with any investigations about incidents unless the requests come directly from our IO.

Hackers can use phishing techniques combined with the uncertainty of how to deal with an incident to obtain sensitive information from employees or contractors. These requests may appear to come from the Regulator, law enforcement, or other authorities – but it is best to send these requests to our IO and let them decide whether they are legitimate or not.

Our employees, partners or contractors should be cautioned not to reply to any requests to cooperate with investigations unless they come directly from our IO.

5.5. ***Protection***. We want to encourage employees, partners or contractors to report incidents and will protect them as much as legally possible to make sure that they are comfortable reporting them.

If an employee, partner or contractor reports an incident in good faith (which means that they did not intentionally cause the incident themselves or help someone else cause it), then we should not threaten them with any recourse or discriminate against them in any way because of their involvement in the incident. We want them to report anything they suspect of being an incident to us and should incentivize them to do so. There should be no recourse against them even if we discover that there was no incident or that the incident did not pose as much of a risk to us as they led us to believe.

We will protect our employees, partners or contractors as much as legally possible when reporting an incident because we want to encourage them to report incidents, provided that they do so in good faith.

5.6. ***Optional anonymity***. If an employee, partner or contractor reports an incident, they may tell us whether or not they wish to remain anonymous.

If they decide that they want to remain anonymous, then the IO will not give their identifying information to anyone else unless absolutely necessary (for example, necessary for law enforcement to proceed with their case).

The IO will keep the identity of an employee, partner or contractor anonymous on request, unless disclosure is absolutely necessary.

6. Verify

We must verify the incident, which means establishing whether an incident has actually occurred or not.

It is a waste of our time to prepare a carefully constructed response unless we have clearly identified an actual incident. We must also make sure that our response is proportional to the incident, which is why we must identify it first – because identifying it entails understanding its scope.

Verify the incident.

6.1. ***Incidents***. An incident is a security compromise or any other related incident where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

This definition has three components:

- **reasonable grounds to believe** – an average person would have thought that there was a security compromise from the circumstances;
- **personal information of a data subject** – the security compromise concerned personal information belonging to a data subject; and
- **accessed or acquired by any unauthorised person** – someone who wasn’t supposed 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 our systems to access data containing personal information;
- **access control failure** – a failure of a password, firewall, or other access control system that allows unauthorised access to personal information;
- **unauthorised use** – of personal information by a member of our personnel;
- **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.

6.2. ***Categories***. Once we have identified an incident, we must work out what category it falls into.

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 suggest a few ways of categorising them – for example, we could categorise an incident based on:

- the **sensitivity** of any information leaked during the incident
  e.g. is it less sensitive information such as names that may be publicly available elsewhere, information of a personal nature vulnerable to misuse, or highly sensitive information like credit card details the wrongful disclosure of which is an offence under South African data privacy law;
- how badly the incident threatens our **reputation**
  e.g. is it a small transgression that we can handle easily or is it something big that could threaten our brand irreversibly;
- how difficult the incident will be to **recover** from
  e.g. is it a simple matter of sending out a well written response or is it a massive problem that needs 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 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 ordinary personal information, special personal information that requires additional protection, or a special class of personal information such as account numbers, special personal information, or the personal information of children;
- how **protected** is the personal information
  e.g. if it was stored on stolen equipment, was that equipment encrypted;
- what has **happened** to the personal information
  e.g. the risk will be potentially harmful to data subjects if equipment has been stolen, but the risk will only be loss of personal information if equipment has been damaged but is still in our 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 even meagre 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 employees, contractors, customers, prospects, or suppliers; 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?

7. Escalations

It is important to escalate incidents appropriately so that they can be dealt with by the appropriate people. Escalation involves taking something more seriously by getting input from a more senior person, which is exactly what we must do to handle an incident properly.

Have the incident properly escalated.

7.1. ***Escalation plan***. We should follow an escalation plan and escalate various categories of incidents to specific people in our organisation when they occur.

This policy does not prescribe an escalation plan. It is something that should be drawn up in consultation with everyone involved in the response team.

Here is an example plan for us to use when drawing up one:

Incident	Report it to
Minor incident	Any member of the office of the IO
Medium incident	Someone that the IO has authorised to handle incidents on their behalf
Major incident	IO
Any other related incident (including emergency situations)	IO

We should have an escalation plan and follow it once an incident has been reported.

8. Respond

We must actually respond to the incident, which is arguably the most important step of all. The cost of an incident is often determined by how well we respond to it.

Respond to the incident.

8.1. ***Resources***. The IO needs to know what resources they have available to them, including what they have access to internally and what they need to get access to externally to deal with security compromises or related incidents.

The IO needs to know what internal and external resources they have available to deal with incidents.

8.2. ***Response team***. The IO should assemble and oversee a response team consisting of representatives from business areas likely to be affected by a security compromise or any other related incident and should consider including representatives from:

- legal;
- human resources (HR);
- information technology (IT);
- any other departments working with personal information; and
- certain external stakeholders or suppliers where appropriate.

The IO needs to decide whether to delegate responsibility to members of the response team.

The IO should clearly document and define the roles of the response team.

Each person should be responsible for different tasks, and they should understand that the IO oversees them.

The IO should have a clear plan of communication within the team.

The IO should assemble a response team to handle security compromises.

8.3. ***Containment and recovery***. Any response to a security compromise or related incident should be backed up by a containment and recovery plan that seeks to limit the damage of the incident.

The plan should specify which member of the response team will lead the containment and recovery process (usually the IO) and establish what each other member of the response team will do in terms of containment and recovery.

Our response should be backed up by a containment and recovery plan.

8.4. ***Notification***. The IO needs to know who to notify in the case of a security compromise, whether it be the Regulator, relevant supervisory authority, data subjects, and law enforcement.

There are legal requirements in terms of POPIA and the GDPR to notify certain parties about security compromises and related incidents that we must comply with when responding to an incident. However, there are also business reasons why we should notify these parties.

The IO should decide whether to notify third parties about a security compromise or related incident. This will give the notification a clear purpose – be it to comply with the law or for our business reasons.

We should notify certain parties about security compromises and related incidents if required to by law or for business reasons.

8.5. ***Notification timeframe***. Section 22(2) of POPIA and Article 33 of the GDPR require us to make notifications as soon as possible after an incident is discovered because:

- Law enforcement needs time to respond;
- We must take reasonable measures to determine the scope of the compromise; and
- We must restore the integrity of our information system.

However, the IO must ensure that they do not compromise the steps set out in this policy by making a notification prematurely.

We must make our notifications as soon as possible after the incident is discovered.

8.6. ***Processor breach notification***. The processor must notify the controller after becoming aware of a personal data breach without undue delay.

8.7. ***Notifying authorities***. Section 22(1)(a) of POPIA and Article 33(1) of the GDPR requires us to notify the regulator or relevant supervisory authority.

We must notify the regulator or supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights of the data subjects.

The purpose of the notification is to allow the appropriate regulatory bodies to perform their functions. It is important that we notify the correct regulatory body. When notifying the regulatory body, we should give details about what we are prepared to do to help them.

We might also need to consider notifying other third parties like law enforcement bodies, insurers, professional bodies, bank or credit card companies, trade unions, and anyone else who can assist in reducing the risk of financial loss to individuals.

The regulator may direct us in terms of section 22(6) of POPIA to publicise the fact that the integrity or confidentiality of our personal information has been compromised if they believe that the publicity would protect an affected data subject.

It is important that we only notify the Regulator where there is a real security compromise or related incident.

We must notify the relevant authorities as required by law.

8.8. ***Notification contents***. The notification must contain at least:

- a breach description, including (i) categories and approximate number of data subjects and (ii) categories and approximate number of personal data records concerned;
- IO (or other contact point) name and contact details;
- likely consequences of the data breach; and
- measures taken or proposed to address the personal data breach and mitigate its possible adverse effects (where appropriate).

8.9. ***Phases exception***. We may provide the information in phases without undue further delay where it is not possible to provide it at the same time.

8.10. ***Documentation requirement***. The controller must document any breaches, by recording:

- the facts relating to the breach;
- the effects of the data breach; and
- and the remedial action taken.

8.11. ***Notifying data subjects***. Section 22(1)(b) of POPIA and Article 34 of the GDPR requires us to notify the data subjects affected by the incident unless their identity cannot be established.

We 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.

We need not notify the data subject in terms of Article 34(3) of the GDPR if:

- we have implemented appropriate technical and organisational measures and those measure were applied to the personal data affected by the data breach;
- we have taken subsequent measures that ensure the high risk to the rights of the data subject is unlikely to materialise;
- unless it would involve disproportionate effort.

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 our website;
- published in the news media; or
- as the regulator may direct.

Section 22(5) of POPIA requires the notification 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 we intend to take to handle the security compromise;
- suggestions of what the data subject could do to mitigate the consequences of the security compromise;
- the identity of the unauthorised person who may have accessed or acquired the personal information (if known to us);

Article 33(3) and 34(2) of the GDPR requires that the communication to the data subject must be in clear and plain language and must:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the IO or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach; and
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

For business reasons, the notification should allow affected individuals to protect themselves. It should also provide advice on how data subjects can mitigate the consequences of the incident and have a mechanism to deal with complaints.

8.12. ***Notifying data subjects (GDPR)***. The controller must communicate the personal data breach to the data subject without undue delay when it is likely to result in a high risk to human beings' rights and freedoms.

The communication must:

- describe the nature of the personal data breach; and
- be in clear and plain language

It must also contain the required information and recommendations, namely:

- our IO's (or other contact point) name and contact details;
- the likely consequences of the data breach; and
- the measures taken or proposed to address the personal data breach and mitigate its possible adverse effects (where appropriate).

The controller need not communicate the personal data breach to the data subject under any of the following conditions:

- they had implemented appropriate technical and organisational protection measures and applied them to the breached personal data, particularly encryption;
- they have taken subsequent measures to make sure that the high risk is unlikely to materialize; and
- it would involve disproportionate effort, provided that they must use a public communication or similar equally effective measure.

The supervisory authority may consider the likelihood of the personal data breach resulting in a high risk where the controller has not already communicated the personal data breach to the data subject and:

- require the controller to communicate the personal data breach to the data subject; or
- decide that one of the communication exceptions has been met and they need not communicate the data breach to the data subject.

We must notify data subjects as required by law.

8.13. ***Notification questions***. It can help to decide when to notify and to what extent to notify the data subject if the IO asks themselves questions, including:

- are we legally or contractually obliged to notify anyone about this incident
  i.e. are there are legal obligations to notify the Regulator and the data subject (there probably are);
- will the notification help the individual data subject
  i.e. bearing in mind the potential effects of the breach, would individuals be able to act on the information provided to mitigate their risks, perhaps by cancelling credit cards or resetting passwords;
- what should we include in our notification to ensure that it is appropriate for the data subjects whose personal data has been breached
  i.e. what is the education level of our data subjects? Is the notification directed at children or adults;
- what are the risks of not notifying the data subject?
  i.e. will they lose trust in us or try to sue us if they find out that we decided not to notify them;
- what are the risks of ‘over notifying’
  i.e. not every incident requires notification of all our customers and leads, and often only the affected subset need by notified.

We must ask relevant questions to decide when to notify and to what extent we should notify.

8.14. ***Manner***. It is important that we frame and deliver our 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, gives the people who were upset more time to control the message, and makes the general public think that we are uninterested in the problem;
- delivering the response as a matter of **urgency** where the fallout is severe
  the first 24 hours are crucial, the Internet does not wait for us to respond, and news will spread with or without our involvement;
- making sure we have formulated our response **properly**
  responding properly means going to the source of the complaints and interacting with the relevant individuals;
- delivering the response on an **appropriate forum**
  take any negative conversations private as soon as possible to reduce the chance of them causing harm through reputational damage; and
- not admitting **liability**
  but still being sympathetic about bad experiences.

We will have successfully responded to an incident if:

- our leadership is accountable;
- we are able to re-establish trust; and
- to provide transparency.

Make sure the response is correctly framed and delivered.

8.15. ***Acknowledgement***. We must acknowledge the security compromise or other related incident, which means to recognise its importance.

To recognise the importance of a security compromise or other related incident, we must collect the following information:

- who or what was affected by the incident;
- why did the incident occur;
- when did the incident occur;
- how did the incident occur;
- to what extent did the incident pose a risk; and
- how did we find out about the incident?

While we should certainly collect all this information, we should also decide whether or not we wish to communicate it all to the affected data subjects who may include our customers or prospects. Certain information must be communicated to affected data subjects by law, but beyond that – communicating information about an incident can help us take ownership of it. But, it can also expose information about it that we may not want to expose.

Ultimately, we should exercise our discretion when deciding how much information to disclose beyond what we are required to disclose by law.

Acknowledge the incident by collecting information about the incident and disclosing appropriate information in our discretion, unless required to disclose it by law.

8.16. ***Apology***. We must apologise for a security compromise or other related incident, which means acknowledging it sympathetically.

An incident causes the people it affects to experience a number of negative feelings, including anxiety, inconvenience, and doubt. It is our job to address these feelings by acknowledging them. This reassures the data subject that we care about the emotional fallout of the incident, which will help resolve it.

The apology should contain an acknowledgement that we are listening to them, seeking answers as to why the incident occurred, and are genuinely sorry. A statement that we are genuinely sorry can buy a lot of time and quell anger and resentment. However, the apology should not amount to admitting liability.

The IO should have a legal representative on their response team for this reason. It is very important that the apology does not focus on us or our organisation. Make the apology about the data subject – they are the ones that matter.

We should apologise to the affected data subjects for the incident – but we must make sure that the apology is genuine.

8.17. ***Action***. We must take action, which means actually sending our response.

Taking action can also mean working out what happened, preventing it from happening again, and maintaining trust with our data subjects – but all these things require us to actually send the response. The IO should handle the security compromise by investigating the problem and identify short and long term solutions in the form of various kinds of responses.

Take action and actually respond to the incident.

8.18. ***Spread***. We must spread what we have already done. It involves using the Internet to our advantage to increase the reach of our response. It is made up of three distinct tactics:

- We must **amplify** the response by directing people to the right information about the incident on the Internet;
- We must find **advocates** to help spread our response in the form of influencers or people that work at our organisation who can be galvanised to carry the message; and
- We need **adhesion**, which involves sticking to our corporate image and values, being clear about what we will and will not do, and sticking to this policy.

We must amplify our response, get advocates, and adhere to our brand, values, and policies in order to spread our response as far and wide as possible.

8.19. ***Other steps***. Other steps we can take as and when needed to effectively respond to a security compromise or other related incident are to:

- get a **media program**, which is a set of press releases and other media content that we can syndicate to the media to help them report on the incident in the best way possible;
- prepare and maintain a **toolkit** to help people in our organisation deal with an incident. Ask our employees and contractors to help develop this toolkit by adding to it when they think it lacks something; or
- the IO should have **template written documents** ready to deploy in the case of an incident, such as letters to the Regulator or other authorities or media statements.

Other steps we can take to respond including getting a media program, making a toolkit, and having template written documents ready to go.

9. Evaluate

A security compromise or other related incident is not over once we have responded to it.

We must evaluate the outcome of that response, which means we need to form an idea of how well it worked. We need to know how well it worked so that we can decide whether an additional response is needed or whether the response we put out is sufficient.

Evaluate our response to the incident.

9.1. ***Analysis***. We must analyse the effects of our response. We can do this by closely monitoring the media to see how our data subjects are reacting to our response.

We then must categorise their reactions and prepare our own content to handle their reactions and send our content to them directly or put it our on the Internet for them to find.

We must analyse our response by monitoring the media.

9.2. ***Answers***. Feedback is the food of champions. We should invite it whenever we can and be grateful for it when our data subjects decide to give it to us.

We must make sure to respond to it where appropriate, but bear in mind that not all feedback needs to be answered. It’s about picking the feedback where our response will have the biggest positive impact on the overall discussion.

The discussion may become hostile, particularly where those giving feedback on the incident are those most severely affected by it. The solution in these situations is to take the discussion private whenever we can.

We can also set the rules of engagement for this feedback response discussion loop by taking control of it.

Answer feedback to our response where appropriate.

9.3. ***Aggregation***. Aggregation involves collecting things together. We should collect everything about the incident together in one place, be it on our website or social media so that our data subjects can find it easily. Aggregating stuff means that we can control the conversation and monitor what results from it.

Collect everything anyone has put on the Internet about the incident together in one place to better control the discussion.

9.4. ***Update policy***. We must update this policy from time to time based on how we have evaluated our responses to incidents and what is happening in our broader industry. This policy does not prescribe an exact update procedure. We must look at how other organisations in our industry have reacted to security compromises and ask what problems they have had, how those problems occurred, and whether they responded to those problems effectively.

Update this policy from time to time based on our evaluation of our responses and what is going on in our broader industry.

9.5. ***Update information security***. We need to update our information security systems based on the outcome of the incident and our response.

Information security is a constantly changing landscape. Section 19(3) of POPIA and Article 32 of the GDPR require us to have due regard to generally accepted information security practices and procedures which may apply to us generally or be required in terms of our industry rules and regulations.

We must update our information security systems based on the outcome of the incident and our response.

10. Questions

Security compromises or other related incidents can be confusing to deal with and we hope this policy has helped to alleviate some of the confusion – but this policy cannot cover all issues when it comes to security compromises or other related incidents.

There will always be issues that fall outside of it and we want people in our organisation to contact the IO with questions when such incidents occur or if they have any questions arising out of this policy.

People in our organisation should contact the IO with any questions about specific incidents or this policy in general.