Security Compromises Policy

1. **OVERVIEW**

1.1. Security compromises require a centralised and swift management and this Security Compromises Policy (**this policy**) outlines a framework for responding to such incidents.

2. **KEY CONSIDERATIONS**

2.1. RETROLEX CONSULTANCY has to comply with the Protection of Personal Information Act 4 of 2013 (**POPIA**) to ensure that measures are taken to keep personal information secure, including specific legal obligations around dealing with a security compromise. Such legal requirements must be observed in addition to the approach set out in this policy.

2.2. RETROLEX CONSULTANCY is also required to comply with POPIA's mandatory security compromise notification requirements, immediately where it acts as operator, or as soon as reasonably possible where it is the responsible party, where there are reasonable grounds to believe that the personal information of any data subject has been accessed or acquired by any unauthorised person/s.

3. **INITIAL IDENTIFICATION, ASSESSMENT AND CONTAINMENT OF ANY SECURITY COMPROMISE**

3.1. An important starting point with any security compromise is to consider what steps are required in order to contain it. For example, if the incident involves a form of intrusion (via either internal or external threats) into RETROLEX CONSULTANCY's systems then containment action could include:

3.1.1. identification of where the intrusion itself is occurring on the systems;

3.1.2. closing down such weak points to contain the incident; and

3.1.3. prevention of further impact on personal information through the compromised systems.

3.2. As part of the investigation it will need to be established exactly what information has been compromised and whether or not the incident took place within the control of RETROLEX CONSULTANCY or whether the risk materialised within the control of its third parties. In the case of third parties, the team will need to assess what obligations and responsibilities may flow under POPIA and also any contract between RETROLEX CONSULTANCY and third parties.

3.3. **Informing Stakeholders:** You should consider which other internal stakeholders should be informed of the incident and at what stage in the investigation process they should be informed (bearing in mind confidentiality and legal professional privilege considerations).

3.4. **Regulatory reporting**: The investigation will require consideration of the reporting requirements under POPIA and other South African ancillary rules. For that, the Information Officer ("**IO**") should be involved from the outset.

3.5. **Confidentiality:** The investigation should also consider keeping the investigation confidential from those (internally or externally) that do not need to be made aware of the investigation (either wholly or in part). This will allow the investigation to continue unhindered particularly with regard to further scoping of the incident and any activity around it. This may include, for example, notifying an appropriate law enforcement authority.

3.6. **Legal professional privilege:** Care should be taken to ensure that any investigation into the security compromise is carried out utilising, to the maximum extent possible, the protection of legal professional privilege. This is particularly imperative where external service providers are procured to carry out containment or investigation.

3.7. **Insurance notification**: The IO and/or the investigation team should immediately, upon becoming aware of a security compromise, notify RETROLEX CONSULTANCY's broker and/or relevant insurer under any applicable cyber insurance policy (or similar policy).

3.8. **Initial containment and assessment**

3.8.1. Do not do anything to the suspected computer/s or other systems equipment, including turning on or off, or shut down the network unless required.

3.8.2. An initial assessment will require the focus on determining factors such as the following (non-exhaustive):

3.8.2.1. What information:

3.8.2.1.1. was impacted by the security compromise (risk materialised therefore high risk)?; or

3.8.2.1.2. could have been subject to impact (risk could have materialised therefore medium risk) as a result of the security compromise?

3.8.2.1.3. Who is affected and what is the likelihood of any harm as a result of the incident?

3.8.2.1.4. Where was the information being processed and handled?

3.8.2.1.5. What was determined to be the cause of the security compromise?

3.8.2.1.6. What was determined to be the extent or reach of the security compromise?

4. SECURITY COMPROMISE NOTIFICATION

4.1. Key Considerations

4.1.1. As a result of the investigations carried out above by RETROLEX CONSULTANCY, in the event that it is reasonably established that there has been unauthorized access or acquisition of personal information of any data subject, RETROLEX CONSULTANCY:

4.1.1.1. is obligated in terms of POPIA to report the security compromise to **the Information Regulator and the data subjects** as soon as reasonably possible after the discovery of the security compromise, taking into account the time it takes to spend on the initial containment, and the legitimate needs of law enforcement;

4.1.1.2. should report to its insurers, in terms of any applicable insurance policy as soon as reasonably possible;

4.1.1.3. must take into account any reporting obligations to other entities or organisations if required by specific legislation - for example, the South African Police Service; and

4.1.1.4. must consider its reporting obligations to other entities or organisations, on an optional basis or if required by any contractual obligation - for example customers or clients, if deemed appropriate by the public relations department, senior management and the IO.

4.2. The team should consider seeking appropriate expert legal advice on the notification requirements.

4.3. Notification to Regulator and Data Subjects in terms of POPIA:

4.3.1. The Regulator must be notified of all unauthorised access or acquisition of personal information of any data subject, as soon as reasonably possible, which notification must include:

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

4.3.1.2. a description of the measures that RETROLEX CONSULTANCY has taken, and intends on taking, to address the security compromise;

4.3.1.3. the identity of the unauthorised person/s (if known); and

4.3.1.4. a recommendation with regards to possible measures that should be taken by affected data subjects to mitigate any possible adverse effects of the security compromise.

4.3.2. Affected data subjects

4.3.2.1. All data subjects whose personal information was accessed or acquired in the security compromise (unless their identity cannot be established), must be notified as soon as reasonably possible, or as directed by the Regulator, after the security compromise incident in terms of POPIA.

4.3.2.2. Notification to the data subjects may only be delayed if the South African Police Service, or the Regulator determines that notification will harm a criminal investigation.

4.3.2.3. As such, the notifications to the South African Police Service or the Regulator will have to be submitted before the affected data subjects, and must include a specific question on whether the notification to the affected data subjects should be delayed.

4.3.2.4. The notification to the affected data subjects must be in writing and communicated to the data subjects in at least one of the following ways:

4.3.2.4.1. mail;

4.3.2.4.2. e-mail;

4.3.2.4.3. placement on the website of RETROLEX CONSULTANCY;

4.3.2.4.4. publication in the news media; or

4.3.2.4.5. as may be directed by the Regulator.

4.3.2.5. The notification must provide sufficient information to allow the affected data subjects to take protective measures against the potential consequences of the compromise. This may include, if known, the identity of the unauthorised person who may have accessed or acquired the personal information.

5. CONTACT DETAILS OF THE IO

Name: Mosa Raju Holomo
Address: 107 Bokmakierie Road, Rooihuiskraal
E-mail address: mosa@retrolex.co.za
Telephone number: 082 997 2487

APPENDIX A

Security Compromises Procedure Flow Chat