**POPI Act Security Compromise Management Guidelines**

**Purpose**

The purpose of this document is to support a high level of assurance of compliance with the POPI Act, condition 7, section 22, “Notification of Security Compromises”. This document should be used in conjunction with other relevant: documented policies and procedures; assessments; audits; best practice guidance; associated with meeting the requirements of condition 7 of the POPI Act.

**Identification of a Security Compromise**

The first step in Security Compromise management is the identification that an incident has taken place. This requires a review of the following:

* What policies and procedures does the organisation have in place to identify and manage the risk of Security Compromises taking place?
  + Those policies and procedures should be followed
* What are the conditions that must be satisfied so that section 22(1) can be invoked (reasonable grounds to believe a security compromise has taken place)?
  + Document the reasonable grounds
* In identifying the Security Compromise can these questions be answered:
  + When did the Security Compromise take place?
  + Which data subjects have been compromised?
  + What were the circumstances of the Security Compromise (accidental, malicious, theft of papers or electronic storage, network breach etc)
* Once the authorised person acting for the Responsible Party is satisfied that a Security Compromise has taken place, then the Notification actions below should follow.

**Notification of the Security Compromise**

In order to comply with section 22 of the POPI Act certain actions must be taken by the Responsible Party:

* Notification to the Regulator – is this required for this Security Compromise? If not, why not?
  + Who will notify the Regulator?
  + How will the Regulator be notified?
  + When will the Regulator be notified?
  + Where will the tracking of the incident be recorded?
* Notification to the Data Subject(s)
  + Who will notify the Data Subjects?
  + How will the Data Subjects be notified?
    - Which approved method will be used?
      * By post
      * By email
      * On he Responsible Party website
      * In the news media
      * As directed by the Regulator
  + When will the Data Subjects be notified?
  + What will be communicated? Must include at least (section 22(5))
    - Possible consequences ot the Data Subject
    - Measures Responsible Party intends to take
    - Recommendation for mitigation by the Data Subject
    - If known, identity of the unauthorised person who may have accessed or acquired the personal information

**Lessons learned review**

It is recommended that after any Security Compromise incident that the Responsible Party should conduct a review which has the following objectives:

* Complete a root cause analysis: why and how did this incident happen?
* Identify actions to minimise a re-occurrence of a similar or related incident. These could include but are not limited to:
  + Changes to policies and procedures
  + Changes to security technical measures (e.g. IT related)
  + Changes to physical security measures
  + Changes to staff training

**Related documentation**

[specify here any related documentation that exists, e.g. policies and procedures]

**Related guidance**

It is recommended that the guidance provided in the IACT-Africa POPI Compliance Toolkit folder Education and Training, sub-folder Security Compromise Management, is reviewed for use in conjunction with this document.