Triple H Cloud Services (Pty) Ltd (THCS)

Information Incident Management Policy and Process

REVIEW SCHEDULE

Date created or reviewed	Version number	Review notes	Person who reviewed
July 2019	V1.00	This document was created in July 2019	Kent Hutchons

TABLE OF CONTENTS

1. Policy Overview

This policy was developed to provide policy direction to guide management and employees of Triple H Cloud Services (Pty) Ltd (THCS) (including contract service providers) in responding to incidents that threaten information privacy or security.

2. Objectives

The objectives of this policy are to:

1. Provide a policy framework for responding to information incidents in accordance with legislative (POPIA) and policy requirements;
2. Consolidate policy by function (information incident management) rather than by business area (security, privacy, records management, etc.);
3. Assist THCS employees and management (including service providers) in understanding their responsibilities in addressing information incidents.

3. Scope

This policy applies to management and employees of THCS (including contract service providers) or any person handling information managed (e.g. collected, accessed, used, shared, stored, disclosed, disposed or archived) by THCS.

4. Supporting Documents

The following documents and tools support the application of this policy:

1. Protection of Personal Information Act no 4 of 2013 (POPIA)
2. Process for Responding to Privacy Breaches
3. Information Security Policy
4. General Incident and Loss Report (GILR)
5. Incident Management Tool (system)

5. Information Incidents

This section defines the steps that must occur in response to an information incident, including the roles and responsibilities of the stakeholders.

An **information incident** is a single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorised by the business owner of that information.

Information incidents include **privacy breaches**, which are a collection, use, disclosure, access, disposal, or storage of **personal** information, whether accidental or deliberate, that is not authorised by the *Protection of Personal Information Act no 4 of 2013.*

5.1 Policy

1. The Information Governance Leadership (IGL) is responsible for the coordination, investigation, and resolution of information incidents.
2. All actual or suspected information incidents must be reported immediately to your departmental Information Process Owner (IPO) and to the Information Officer using the Information Incident Management Process/System.
3. The Information Officer is solely responsible for liaising with the Information and Privacy Regulator regarding an actual or suspected privacy breach. The only exception may occur in case of a Whistle Blower provision which allows for information sharing with the Regulator by an employee acting in good faith.
4. Information Governance Leadership will be responsible for decisions relating to notifications when a decision must be made to not notify individual(s) based on a balance of harms.

5.2 Process: Event Reporting

1. Any employee, service provider or other person who discovers a suspected or actual information incident (including privacy breaches) must immediately report it to their IPO or designated management contact (if one has been appointed). The incident/event must be recorded in the incident management system / tool.
2. Where the incident will have high impact on the business, the IPO or management contact, must immediately report the information incident to the Information Officer.
   In circumstances where the IPO or management contact is not immediately available (in person or by phone) or the employee / contractor does not have access to the information management system, the employee, service provider or other person must immediately report the information incident directly to the Information Officer.
3. Where the incident will have high impact on the business, the Information Officer contacts the information incident reporter to:

   - Assess and document the information incident including, if applicable, the nature, sensitivity, volume, impact and type of incident (physical and/or information);
   - Assist with resolving the incident and containing the information incident (if applicable) if it is still ongoing; and
   - Provide the information incident reporter with instructions explaining the incident response process and priorities (e.g., contain the loss, prevent a recurrence, and determine next steps).

   The Information Officer decides if additional information should be gathered to determine the response strategy and to define work assignments according to relevant factors, including:

   - Type of information incident (physical and/or information);
   - Nature and sensitivity of the incident;
   - Volume; and
   - Impact and implications of unauthorised disclosure or asset loss.

4. The Information Officer determines whether the information incident is major or minor, based on relevant factors that include:

- The incident involves personal or sensitive information;
- Whether there is, or could have been, a reasonable expectation of harm to any individuals as a result of the incident;
- Whether individuals will be, or have been, notified that their personal information was breached;
- Whether the incident will be, or has been, reported to the Information Regulator; or
- Whether the incident has a serious or potentially serious public impact.

Minor information incidents:

- The Information Process Owner (IPO) will be the main point of contact for the breach.
- The IPO will refer all minor information incidents to the Information Officer for follow-up and resolution in collaboration with the business owner.
- Information Officer requests the IPO to provide a report regarding the privacy breach.

Major information incidents:

- The IPO coordinates an incident management and investigation process in order to conduct an assessment and gather evidence.
- Status reports are sent to the Information Officer who provides periodic updates to the Information Governance Leadership (IGL) where appropriate and as needed.

Where the root cause of the privacy breach has a major impact on the business, change management must be initiated.

- The Information Officer has to ensure that the information breach is reported to the Information Regulator.

5.3 Notification of Affected Individuals

The impact of privacy breaches must be reviewed to determine if it is appropriate to notify individuals whose personal information has been affected by the breach. The IPO will work with the Information Officer to notify affected parties and take other required actions as appropriate.

The key consideration in deciding whether to notify an affected individual is whether it is necessary to avoid or mitigate harm to an individual, such as:

- A risk of identity theft or fraud
- A risk of physical harm
- A risk of hurt, humiliation or damage to reputation or
- A risk to business or employment opportunities.

Other considerations in determining whether to notify individuals include:

- Legislative requirements for notification;
- Contractual obligations requiring notification;
- A risk of loss of confidence in the public body and/or good customer/client relations dictates that notification is appropriate.

Notification is determined based on the balance of harms. Under this principle, an individual(s) who could potentially face harm as a result of an information incident may not be notified if it is determined that the harm that would result from conducting notification would outweigh the benefit to be gained from the notification.

Important: Where an information incident involves the potential for significant harm to an individual(s), the decision to not notify individual(s) is based on the balance of harms and must be approved by the Information Governance Leadership Committee.

If it is determined that notification of individuals is appropriate:

- Notification should occur as soon as possible following the breach and
- Affected individuals should be notified directly, whenever possible.

5.4 Closure of information incident file

When closing an information incident file, the Information Officer notifies the process owner and Information Governance Leadership. The Information Officer writes a final report, including recommendations, and submits it to required stakeholders. There are two types of recommendations included in final reports:

- essential recommendations, which must be implemented (change management); and
- advisory recommendations, which the organisation decides whether to implement (the IGL informs IT Steering Committee, Exco and the Board of the decision).

5.5 Compliance

- The organisation as a whole or the business owner, as applicable, will be responsible for implementing the final report's recommendations and reporting their status; and
- The business owner / sponsor will report the results to Information Governance Leadership.
- The Information Officer may perform compliance reviews or may audit the implementation of the recommendations and its effectiveness.

5.6 Responsibilities

5.6.1 Employee

In the case of the actual or suspected incident, the employee's responsibilities are to:

- **Report** – the information incident immediately to their IPO or the Information Officer;
- **Recover** – the confidential or personal information if possible, or otherwise contain the incident to lessen the impacts and implications for the organisation and individuals. (Note: If the incident involves information technology, seek the direction of the IT manager before taking any containment steps).
- **Remediate** – the information incident by working collaboratively with the process owner and Information Officer or others to determine the specifics of the incident and resolve it.
- **Prevent** – information incidents by being diligent in the handling of confidential or personal information, and being an active participant in developing the culture of prudent information management.

5.6.2 Information Process Owner (IPO)

In the case of the actual or suspected incident IPO's responsibilities are to:

- **Report** – receive the report about the information incident from the employee and provide direction on assessing the incident and ensuring it is recorded in the incident management system.
- **Recover** – determine if the confidential or personal information can be recovered, or if the loss/disclosure can otherwise be contained. (Note: If the incident involves information technology, seek the direction of the IT Manager before taking any containment steps).
- **Remediate** – work collaboratively with the Information Officer or others to determine the specifics of the information incident and to implement the steps needed to resolve it.
- **Prevent** – information incidents by:

- Implementing recommendations from the Incident Report and ensuring that employees know and understand how to apply changes in the handling of confidential or personal information.
- Participating in the development of a culture for the prudent management of information, including by providing training.
- Ensuring employees understand their responsibility in reporting all actual and suspected information incidents, including containing the loss and/or recovering the information.
- By notifying individuals or parties affected by the incident, where directed.
- Ensuring Contractors and Service Providers understand their responsibilities under the Information Incident Report Process and working with them to ensure timely and accurate reporting.

5.6.3 Contractor or Service Provider

In the case of an actual or suspected information incident, the contractor's responsibilities are to:

- **Report** – Contractors will ensure that any of their employees, service providers, or other persons who discovers a suspected or actual information incident (including privacy breaches) immediately notify their IPO or manager and report it to the organisation's contract manager.
- The contract manager is then required to immediately record the information incident in the information management system.
- **Recover** – the confidential or personal information if possible, or otherwise contain the incident to lessen the impacts and implications for the business and individuals. (Note: If the incident involves information technology, seek the direction of the Contract and/or IT Manager before taking any containment steps).
- **Remediate** – the information incident:
  - With the organisation's Contract Manager as the incident owner.
  - By working collaboratively with the contract manager and the Information Officer.

- By supporting the investigation and Information Officer, or others to determine the specifics of the information incident and resolve it.
- By notifying individuals or parties affected by the incident, where and as directed by the Information Officer and the contract manager.

- **Prevent** – information incidents by:
  - Ensuring that employees know and understand how to apply changes in the handling of confidential or personal information.
  - Being diligent in the handling of confidential or personal information.
  - Implementing recommendations from the Information Incident Report Process and reporting the results the Information Officer.
  - Developing a culture for the prudent management of information, including by providing training.
  - Ensuring employees understand their responsibility in reporting information incidents, including containing the loss and/or recovering the information.

5.6.4 Information Officer

- Responsible for the coordination, investigation, and resolution of all information incidents, including privacy breaches.
- Receives and reviews status reports and, where applicable, final information incident investigation reports and reports on implementation of recommendations.
- Ensures that the recommended controls of the final report are appropriately implemented through audits.
- Reports information incidents to the Information Governance Leadership of the organisation
- Contacts responsible stakeholders to ensure appropriate communication, recommendation, and collaboration, where appropriate.
- Liaises with the Information Regulator on privacy breaches, where appropriate.