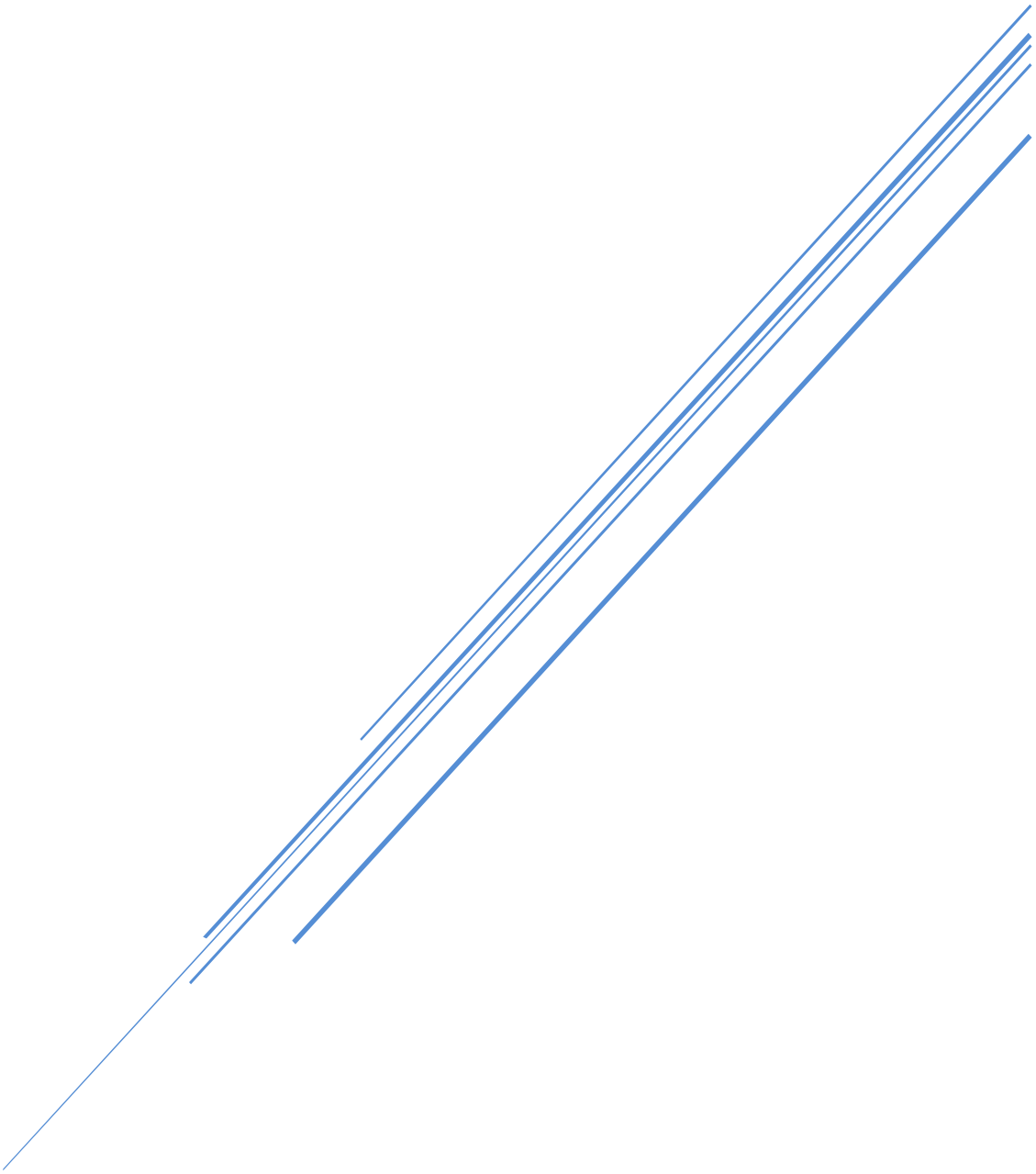
SECUREKLOUD

Incident Management Procedure



Revision Chart				
Version	**Author(s)**	**Reviewer(s)**	**Description**	**Date**
1.0	Sasikumar N R	Raj / Ravi	Original Version	10/Oct/2017
2.0	Sriram	Ravi	Name Conversion	06/Jan/2021
3.0	Silambarasan	Sriram	Version Update	06/Jan/2022
4.0	Silambarasan	Sriram	Version Update	11/Oct/2023

Table of Contents

Objective 3

Scope 3

Methodology 3

- Responsibilities and procedures 3
- Reporting information security events 3
- Reporting information security weaknesses 4
- Assessment and decision on information security events 4
- Response to information security incidents 4
- Learning from information security incidents 4
- Collection of evidence 4

Objective

To ensure information security events and weaknesses associated with information systems are communicated in a timely manner and ensure the corrective actions to be taken properly.

Scope

The methodology is applicable to all the security systems in SecureKloud Technologies Ltd premises, where the information is received, processed, and used. It is applicable to all soft, hard and voice information.

Methodology

Responsibilities and procedures

The overall responsibility for processing information security incidents rests M.R and ISMS team. Based on the impact of the incident, team decides the resolution procedure. The escalation procedure to be followed for reporting different categories of incidents is detailed in the format annexed.

Reporting information security events

Security incidents are defined as events that could cause unauthorized disclosure, modification, or destruction of organizational information assets, or loss or destruction of the physical equipment associated with the computer systems and it's peripheral or network infrastructure components. Security incidents also include other aspects of security, such as carrying firearms, other lethal weapons on the organization property, areas typically secured being left unlocked or unattended, fire or hazardous material spills, witnessing someone performing an unsafe act and committing a violation of security policies or procedures etc.

All users in SecureKloud Technologies Ltd are responsible to report any such observed or suspected security incidents.

Reporting information security weaknesses

Security weaknesses are defined as loopholes, weak points or vulnerabilities in a software application. These vulnerabilities or the loopholes may be exploited to gain unauthorized access to data or systems.

All users in SecureKloud Technologies Ltd are responsible to report any such observed or suspected security weaknesses.

Assessment and decision on information security events

All information security events reported in SecureKloud Technologies Ltd are assessed and decided whether they can be categorized as security incidents based on the number of users affected and the impact of the event.

Response to information security incidents

Reported incidents are attended by the concern personnel, who has been assigned for each incident as per the ticket number allotted.

Learning from information security incidents

All information security incidents reported in SecureKloud Technologies Ltd are documented and stored in the Corrective and Preventive Actions Database. The team consolidates the incident reports for root cause analysis. The team considers these as an input for appropriate actions and necessary controls to avoid reoccurrence of the incidents. As a part of improvement, the relevant stakeholders are communicated.

Collection of evidence

SecureKloud Technologies Ltd has identified all applicable laws and regulations. When a follow-up action against a person or organization after an incident involves legal action, the records and documents that can be accepted as evidence are collected and maintained.

It is ensured that all evidence collected in the process is:

1. Admissible as evidence – Acceptable to court and legal authorities
2. Complete – Present a complete trail of the incident
3. Meet quality requirements – Are readable, legible etc.

Details of the Incident	**Ticket number allotted**	**The Notification Process**	**Technical Details / Fix Actions**	**Conclusion**	**LOG**
° Specifically, what caused the incident (Who, what, where, when, how)?		° Include every step in the notification process ° Automated monitoring notification ° An infrastructure team member noticed something out of the ordinary ° Detail flow of the incident response °Communication of resolution of the outage	° Specific details of troubleshooting ° Specific changes (configuration, hardware, etc.) ° Steps to confirm the outage was resolved ° Ticket numbers	° What was the basic cause of the incident? ° What could have prevented this? ° Impact (none, degraded performance, downtime) ° Business criticality (revenue producing, business critical, low) ° Estimated cost (impact + business criticality) ° What prevents the incident from reoccurring? ° What additional actions or research need to happen	° Logs or error messages ° Contents of trouble tickets ° Contents of e-mail