Information Security Incident Management Procedure

KG Invicta Services (KGiS)

[Ref: ISM-PLC-DOC-05]
[Ver: 1.0]
[05th April 2023]
[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiS Campus, Thudiyalur Road, Saravanampatti, Coimbatore - 641035, India

www.kginvicta.com

Statement of Confidentiality

This document contains confidential and proprietary information of KG Invicta Services Private Limited (KGiS). It is furnished for KGiS internal use and purpose only. Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose. This document is reviewed at least annually.

Copyright and Intellectual Property

a. KGiS logo are registered marks of KG Invicta Services Private Limited.

b.

Table of Contents

1 Document Control

1.1 Document Owner and Approval

KGiS's Information Security Office (ISO) is the accountable owner of this procedure. The ISO is responsible for ensuring that this document is reviewed periodically by the relevant stakeholders in line with the review requirements of the Information Security Management System (ISMS).

A current version of this document is available to all KGiS members at the corporate Intranet and is published on 05th April 2023.

This procedure document was approved by the Head of ICT on 05th April 2023 and met the required Documentation Quality Standard and is issued on a version-controlled basis under the signature.

Name: Shanmugam C

Designation: GM - ICT

Signature: Date:

1.2 Amendment History Record

Version	Description of Change / Action	Resource	Date
1.a	New draft baseline of ISMS procedure	Harikrishnan P	05th April 2023
1.0	Verified and Approved By	Shanmugam Chinnasamy	05th April 2023

1.3 Cross References

All reference documents available in – Shared Folder
ISO 27001– Information technology – Security Techniques – Information security – Requirements
ISO 27002 – Information technology – Security techniques – Code of practice

1.4 Document Sign off and Distribution

Name	Designation	Signature	Version	Date
Shanmugam Chinnasamy	GM- ICT		1.0	05th May 2023

Document Distributed for Internal Approval.

Stakeholder	Date
All Head of Departments and Departments	

2 Definitions & Glossary

Term	Definition
Confidentiality	Prevention of unauthorized access by people, resources, and processes to information.
Integrity	Prevention of intentional or accidental unauthorized changes to information.
Availability	Assurance that information is accessible by authorized users whenever needed.
Information Security Incidents	An information security incident is an event that impacts on the confidentiality, integrity or availability of an information system or network, through an act that compromises business operations of KGiS ICT. Additionally, it refers to an act of violation or imminent threat of violation to computer security policies, acceptable use policies, or standard security practices.
Incident Response Team (IRT)	A group of people who respond to an incident. The team is constituted by Information Security Officer based on the nature and criticality of the incident.
Security Incident Management Database (SIMDB)	A database containing all details of an incident including its description, its impact on business, root cause analysis, supporting evidence, corrective/preventive measures deployed, and a synopsis of the actions taken from the reporting of an incident to its closure.
Root Cause Analysis	Root cause analysis is a problem-solving method used to identify the root cause of a problem rather than merely addressing the immediately obvious symptoms. By taking into account preventive measures to a root cause, likelihood of incident recurrence can be minimized.
IS Officer	Information Security Officer
ISO / IEC	International Organization for Standardization / International Electro technical Commission
Information	Information is an asset which can exist in many forms such as printed or written on paper, stored electronically, transmitted by post or by using electronic means, or spoken conversation and has a value to an organization.
Information Security	The act of protecting information that may exist in any form mentioned above from unauthorized access, use, disclosure, disruption, modification or destruction, with the objective of ensuring business continuity, minimizing

	business risk, and maximizing return on investment and business opportunities.
Users	User is an individual, including all the employees of KGiS and vendor or third-party contractor, who has access to the information and information processing facilities of KGiS ICT and uses it for his/her day-to-day activities.
Information Asset	An information asset is any information or information processing facility that has value to KGiS ICT.

3 About the Document

3.1 Introduction

The Information Security Incident Management Procedure is a critical component of an organization's overall information security framework. It provides a structured and systematic approach for identifying, responding to, and managing security incidents that may compromise the confidentiality, integrity, or availability of sensitive information and critical systems.

This introduction aims to provide an overview of the Information Security Incident Management Procedure and its importance in protecting organizational assets from cyber threats and unauthorized access. It outlines the objectives, scope, and benefits of implementing a robust incident management process, highlighting the significance of timely incident detection, effective response, and continuous improvement. By establishing a well-defined incident management procedure, organizations can mitigate risks, minimize the impact of security incidents, and maintain the trust and confidence of stakeholders in their ability to protect sensitive information.

Furthermore, this introduction emphasizes the importance of a proactive and holistic approach to incident management, fostering a culture of security awareness, continuous monitoring, and ongoing improvement. By implementing an effective incident management procedure, organizations can effectively respond to and recover from security incidents, learn from past experiences, and strengthen their overall security posture.

3.2 Objective

The objective of this procedure is to enables KGiS to effectively respond to security incidents, mitigate risks, protect sensitive information, and maintain the trust of stakeholders. It enables organizations to minimize the impact of incidents, learn from them, and continually enhance their security practices to stay ahead of emerging threats.

3.3 Scope

This procedure applies to all information assets management owned or managed by the KGiS ICT staff (permanent, contract employees, and students), and external parties (contractors, consultants, vendors, suppliers, partners and customers)

3.4 Roles and Responsibilities

- Head of ICT is responsible to review and approve this procedure and to ensure that it reflects the current requirements.
- The Information Security Officer is responsible for development, implementation, maintenance, and enforcement of the procedure.
- Service Desk is responsible for:
    - Identification of security incidents.
    - Assigning reported security incidents to the concerned engineers.
    - Classifying information security incidents.

    - Performing initial security incident analysis.
    - Taking measures for immediate containment of security incidents.
    - Keep users informed on the status of reported incidents.
- The Incident Response Team (IRT) is responsible for:
    - Performing incident analysis.
    - Timely escalation and coordination with vendors/external agencies.
    - Taking corrective measures to contain security incidents.
    - Providing regular updates about incident containment to IS Officer.
- Information Security Officer is responsible for:
    - Development, implementation, maintenance and enforcement of this procedure.
    - Constituting and supervising the incident response team (IRT).
    - Providing support and guidance to the IRT during incident response.
    - Engaging external security agencies during incident response.
- ISMS internal audit Team is responsible for conducting regular audits to ensure compliance to this procedure.

4 Procedure

The processes that need to be followed for the effective implementation and management of this procedure are explained in this section. Information Security Incident Management Procedure aims at describing the steps to be followed at time of incident detection. The various stages of incident management are as follows:

- Incident Reporting
- Incident Validation
- Incident Response
- Incident Closure

4.1 Incident Reporting

- All employees and non-employees (referred to as users) should report suspected or actual security incidents to Service Desk Solution.
- Automated Security Events from SIEM, Anti-virus, Anti-malware other security devices shall log security incidents through Service Desk Solution.
- Examples of information security incidents may include the following but not limited to:
    - Non-compliances with security policies, procedures or standards
    - Virus alerts
    - Password sharing or compromise.
    - Access violations
    - Information leakage or loss
    - Misuse or unacceptable use of information assets
    - Loss of equipment or facilities
    - Breaches of physical security arrangements
- After being notified of the security incident, Service Desk should assign engineers using Service Desk Solution.

4.2 Incident Validation

- When a security incident is assigned, the engineers should perform a preliminary analysis of the incident. As part of this analysis, the engineers should also contact the user who reported the incident to gather any additional details.
- If the issue reported is a valid security incident, the engineer should check the priority of the ticket.

- The engineer should also review if the category selected is accurate and if not, re-categorize the ticket.
- Once categorized, the engineer should inform the Information Security Officer about the incident. The IS Officer, after reviewing the nature of the issue, decides if users need to be informed. When users need to be informed, the IS Officer should alert the Service Desk to send the appropriate communications. IS Officer should also provide Service Desk with relevant instructions to be included in the communication.

4.3 Incident Response

- After ascertaining the priority of the security incident, the engineer should take steps to contain the incident and bring any damage under control.
- Once contained, the engineers should inform the IS Officer. The IS Officer in coordination with section heads should then inform the relevant departments, as needed. If services offered to users are affected, the IS Officer may decide to inform users as well. In such cases, a formal communication should be initiated from Service Desk. If external users too need to be informed, the Service Desk should notify the ICT Manager.
- Once the incident is contained, the IS Officer should be informed, and the ticket should be assigned back to Service Desk for closure.
- If additional resources from other sections or departments are required for containing the incident, the engineer should initiate a request to IS Officer.
- Based upon the required effort in terms of people, tool etc., the IS Officer should form the IRT to work on and contain the incident.
- The IRT should investigate the incident and take immediate steps to contain and correct the incident.
- The IRT should involve vendors and service providers, as may be necessary, while containing the incident.
- The IS Officer, if deemed necessary, should engage external security agencies as part of containment. External security agencies may include specialist incident response teams such as Computer Emergency Response Team, Tamil Nadu Police, etc.
- The incident, if not contained and corrected within the pre-defined timeframes, should be escalated as per Incident Management Escalation. The IS Officer should support and supervise the IRT during the entire incident response exercise.

4.4 Incident Closure

- The closure of all requests is done at Service Desk by changing the status of the ticket to 'Closed'.
- Service Desk should initiate root cause analysis by creating a problem ticket.

4.5 Roles and Responsibilities Matrix

Roles/ Responsibilities	User	Service Desk	Engineer	IRT	Information Security Officer
Incident Reporting	R	I	R		
Incident Classification		R	R,A		
Incident Response	C,I	I	R	R	A,C,I
Closure	I	R		C,A	

R Responsibility – The personnel who is responsible for performing the task.

A Accountability – The personnel who is accountable for the process or data.

C Consulted – The personnel who provide opinions or suggestions.

I Informed – The personnel who should be informed with the progress and updates.