Corrective and Preventive Action Procedure

KG Invicta Services (KGiS)

[Ref: ISM-PLC-DOC-02]

[Ver: 1.0]

[05th April 2023]

[Classification: Internal]

+91 422 4419999

KGiS
o 365, KG Invicta Services Private Limited KGiSL 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 Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose.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	04th 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
ISO / IEC	International Organization for Standardization / International Electro technical Commission.
Root Cause Analysis	Root cause analysis is a set of problem-solving methods aimed at identifying the root causes of an incident/event. Root cause analysis results in elimination of the root causes instead of solving it to contain the current situation.
Preventive Action	A preventive action is a planned control implemented to eliminate the cause of potential non-conformities, that may be foresighted during a management review, risk assessment, performance measurement etc in order to prevent their occurrence.
Corrective Action	A corrective action is a planned control implemented to eliminate the cause of non-conformities that may rise due to violation of any management system controls, requirements, customer complaints, incidents or weaknesses etc. in order to prevent their recurrence.
Confidentiality	To ensure that data/ information is not made available or disclosed to unauthorized individuals, entities
Integrity	To ensure accuracy and completeness of the data/ information is maintained. Modifications to the information is made only by authorized individuals
Availability	To ensure that data/ information is made available, accessible, and usable for authorized personnel.

3 About the Document

3.1 Introduction

The Corrective and Preventive Action (CAPA) procedure is a crucial component of any organization's quality management system. It provides a systematic approach to identifying, investigating, and addressing nonconformities, incidents, and potential issues. By implementing CAPA procedures, organizations can effectively address problems, eliminate root causes, and prevent their recurrence, ultimately driving continuous improvement and ensuring customer satisfaction. This introduction aims to provide an overview of the importance of CAPA and its role in maintaining a robust quality management system.

3.2 Objective

The objective of this procedure is to outline and establish a process in KGiS's to identify, implement proactive measures that address the root causes of identified problems, nonconformities, or incidents. Corrective and preventive actions aim to eliminate the cause of the issue to prevent its recurrence in the future.

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 responsible for reviewing and approving the procedure and ensuring that it reflects the current requirements.
- The Information Security Office are responsible for
  - Providing required support during implementation of corrective and preventive controls
  - Reviewing the status of reported corrective and preventive actions
- ISMS Process Stakeholders are responsible for
  - Ensuring adherence to this procedure
  - Ensuring that root-cause analysis is conducted in respective processes and the result is taken as input to take corrective & preventive action.
  - Ensuring corrective and preventive actions are identified.
  - Implementing corrective and Preventive actions
  - Tracking implementation status of planned controls.
  - Keeping internal team informed on status of implementation.

4 Procedure

The processes that need to be followed for the effective implementation and management of this procedure are explained in this section.

4.1 Identification

- Non-conformities may get identified in an Information Security Management Systems due to any of the following (but not limited to):
    - Internal Audit findings
    - Performance measurement reports
    - Deviation from the policies and Procedures
    - Violation to any applicable legal or regulatory requirements.
    - Management Review
    - Feedback from supplier, contractors or other interested parties associated with KGiS ICT Department.
    - New vulnerabilities or threats identified which were not addressed in previous cycle of risk assessment.
- Above sources of non-conformities are identified as a part of specific processes/activities established in KGiS ICT Department. The concerned process owner/stakeholder should ensure that such non-conformances are handled in appropriate manner.
- Whenever such non-conformances are identified, concerned process stakeholders should perform further analysis/investigation to find out the root cause of the non-conformity.
- Once the root cause of the non-conformity is identified, further action of recording the same in a formal manner should be performed by different process stakeholders as a part of this procedure and as defined below.
- If an action is planned on the basis of a potential non-conformity without any actual issue, root cause is not required.

4.2 Recording

- Based upon the inputs from different processes during identification phase, suitable path of action is chosen as a part of this process.
- If a non-conformity is detected in the existing processes/activities and corresponding root cause analysis is already performed, following steps should be clearly defined using the CAPA form:
    - Source of the non-conformity e.g. Incident management, Internal audit, Performance measurement etc.

- Description of non-conformity
- Result of root cause analysis
- The corrective and preventive action required for solving the non-conformity.
- Responsibility to implement the corrective and preventive action.
- Target date to close the implementation of corrective action.

- The above details should be identified by the concerned process stakeholders as defined in specific processes/activities.
- The corrective & preventive action (planned controls) should identify the best possible solution to mitigate the risk/problem highlighted in specific processes/activities. The solution should be selected considering the following:

  - Risk should be mitigated up to the acceptable level of risk.
  - Resource requirement to implement the control.
  - Cost/Benefit of implementing the planned control.
  - Any alternative available which can partially mitigate the risk and KGiS ICT can accept the residual risk.

- The target dates identified for implementation of the planned controls should be realistic considering the above parameters.
- The process owners should verify the details and approve the corrective/preventive action. The action taken should be appropriate to the magnitude of problem/risk identified/evaluated.
- The records of all such corrective and preventive action should be maintained by the respective process stakeholders for future reference/verification.

4.3 Implementation

- Once the planned corrective or preventive action is approved by the process owner of respective processes, the process stakeholders should initiate the implementation process.
- The processes stakeholders, wherever deemed necessary, should gain support from respective department/section or other relevant department/section while implementing the planned control.
- The process stakeholders should obtain approvals from the process owners for corrective/preventive action which cannot be implemented within the above specified time limits.
- The process stakeholders should ensure that the necessary resources required for implementing the corrective/preventive action are obtained in advance from the management e.g. manpower, budget, tools etc.
- On completion of the implementation, the planned corrective/preventive action should be verified by the process owner for its effectiveness and comprehensiveness.
- Process Owners may ask for any evidence to be gathered to confirm the fulfilment of the implementation.

4.4 Tracking and Closure

- As a part of the implementation, the process stakeholders should keep concerned process owners updated about the implementation status. If required as a part of specific processes/activities, the process stakeholders may need to submit periodic status report to the process owner.
- The process stakeholders should communicate any delays or difficulties in implementing the corrective & preventive action to the Information security officer and ISSC within the permissible timeline.
- The process stakeholders should provide justification for any delays in implementation to the concerned process owner.
- The implemented corrective/preventive action may be verified by the internal audit team as a part of next internal audit cycle to ensure its effectiveness & comprehensiveness.
- The implemented corrective/preventive action may be taken up as an update for next ISMS Committee Meeting meet based upon the criticality of the issue.

4.5 Roles and Responsibilities Matrix

Roles/ Responsibilities	Process Stakeholder	Process Owner	ISSC
Identification	R	A,C	I
Recording	R	A,C	I
Implementation	R	A,C	I
Tracking	R	A,C	I

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

5 Record Template

Following are the records that get developed as a part of this process - Corrective & Preventive Action Form

CAPA Template.xlsx