Information Security Organization Charter

Doc Ref: ISM_Gen_01_ Information Security Organization Charter

Version: 1.0

05th April 2023

Classification: Internal

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 Except with a prior written permission of KGiS, this document and the information contained herein may not be published, disclosed, or used for any other purpose.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

Document Control			
Issue / Rev.	**Date**	**Prepared by**	**Title**
0.1	08.01.2023	KGiS	Information Security Organization Charter
1.0	04.04.2023	KGiS	Updated the members

Revision History			
Version No.	**Date**	**Status / Remarks**	**Prepared By**
0.1	08.01.2023	Draft	Harikrishnan P
1.0	05.04.2023	Final	Shanmugam C

Approved by:

GM -ICT

Table of Contents

1. Overview

A management framework has to be established to initiate and control the implementation of Information Security Management System (ISMS). This charter document provides the list of roles and responsibilities w.r.t information security for KGiS. Level of involvement of different roles is defined as per the following.

Responsible	Those who are responsible for the completion of a task, project, or deliverable.
Accountable	Those who are answerable for the correct, thorough and successful completion of all work actions needed to achieve a task, project, or deliverable. Typically there is only one role with a participation type of “Accountable.”
Consulted	Those whose opinions are sought concerning activity related to a task, project or deliverable
Informed	Those who are kept up to date on the progress of a task, project, or deliverable.

2. Purpose

The purpose of this charter is to provide clear management directive on creation, management and functioning of the Information Security Steering Committee (ISSC), Chief Security Officer/MR, the Internal Audit Team (IAT) and the respective teams in KGiS for the implementation of ISMS. This charter document provides the Roles and Responsibilities of the various Teams at KGiS in the ISMS Implementation.

3. IT Management Organization

The fundamental step in implementing ISMS is to establish an Information Technology Management Organization. As a part of this, the following teams have been identified at KGiS to be part of its IT Management Organization.

- CEO/ Managing Director
- General Manager - IT
- Information Security Steering Committee (ISSC)
- Head of Information Security
- Group Head -Compliance
- Compliance

- Head of Department
- Information Security Champions
- Internal Audit Team
- Security Incident Response Team (SIRT)
- Employees

4. Boards of Directors

Position: Executive Chairman	
Activities	Level of Involvement (RACI)
Accepting the responsibility of ISMS within KGiS and presenting commitment towards it.	Accountable
Overseeing a properly managed and implemented information security program/management system and review risk assessment reports	Accountable

5. ICT - General Manager

Position: ICT -GM	
Reports to – Executive Chairman	
Activities	Level of Involvement (RACI)
Accepting and endorsing the overall responsibility of ISMS within KGiS and presenting commitment towards it	Accountable
Enforcing organization wide Information Security Management Systems.	Accountable
Enforcing the implementation of ISMS Policies and Procedures across KGiS.	Accountable
Overseeing and monitoring compliance to the ISMS related Policies at KGiS and review the risk assessment reports. Accountable Enforcing accountability towards Information Security.	Accountable
Enforcing accountability towards Information Security	Accountable

6. Information Security Steering Committee

Position: ISSC	
Reports to – Executive Chairman	
Frequency of Meeting – Yearly	
Quorum - The Quorum to convene a meeting shall consist of at least three quarters of the members	
Members	
• Shanmugam Chinnasamy • Harikrishnan P • Rajeshwar C • Govind Rajagopal • Hariharan V • Gautham N • Shyam Sundar A • Ashokachackravarthi S	
Activities	Level of Involvement (RACI)
Supervise and ensure the implementation of the ISMS controls across KGiS.	Responsible
Align Information Security to the strategic direction	Accountable
Promote an Information Security culture	Accountable
Review, maintain and approve the ISMS Policies and Procedures periodically and ensure their implementation.	Accountable/ Responsible
Enforcing accountability towards Information Security	Accountable
Review and approve the Risk Assessment Methodology and the results of the Risk Assessment.	Accountable
Make recommendations for both corrective and preventive actions.	Accountable
Ensure that adequate resources are provided to implement and support the ISMS implementation including the establishment of the Information security Champions Team.	Accountable
Ensure KGiS's Information Security program covers all business units and resources and any new initiatives in information technology.	Accountable/ Responsible
Follow up and Review the Internal and External Audits conducted.	Responsible

Review Information Security incidents and ensure appropriate actions are taken on time.	Responsible
Review and approve exceptions to the ISMS Policies.	Accountable
Conduct periodic reviews on the implementation of the ISMS on the performance of the ISMS and its controls, report to the management on the same.	Responsible
Ensure the integration of Information Security within business and the other management frameworks in place.	Accountable
Ensure the recommendations approved by the committee are implemented	Accountable
Additional to the above following points from ISMS shall also be discussed as applicable. • customer feedback • service and process performance and conformity. • current and forecast human, technical, information and financial resource levels. • current and forecast human and technical capabilities. • Cyber Security risks. • results and follow-up actions from audits. • results and follow-up actions from previous management reviews. • status of preventive and corrective actions. • changes that could affect the ISMS. • Opportunities for improvement. • Records of management reviews shall be maintained.	Accountable

7. Head of Information Security

Position: Head of Information Security	
Reports to – ISSC Committee	
Activities	Level of Involvement (RACI)
Plan, implement and maintain an information security program/management system that is integrated with the whole entity's processes.	Responsible

Coordinate with senior management to identify the Information assets (in consultation with the information security Champions Team) and develop the Information Assets Register.	Accountable
Plan, develop, update and periodically review the Risk Assessment Methodology along with senior management in the entity.	Responsible
Report to the ISSC on the summary of the Risk Assessments.	Accountable
Ensure that the appropriate operational controls based on the outcome of the Risk Assessment are selected and implemented.	Responsible
Develop necessary ISMS Policies and Procedures based on risk assessments.	Responsible
Ensure periodic review of the ISMS Policies and Procedures.	Accountable
Plan periodic Information Security training and awareness exercises.	Accountable
Monitor Information Security incidents and report on the Information Security incidents to the ISSC	Responsible
Ensure and review compliance to the ISMS and report any non-compliances to the ISSC, including Audit and assessment reports.	Responsible
Ensure review of third-party contracts, SLAs and access to KGiS's computing resources and facilities	Responsible
Review exceptions to the ISMS Policies and recommend them for approval/ rejection to the ISSC.	Responsible
Liaise and maintain contact with law enforcement authorities, regulatory bodies, security groups and industry forums in the field of Information Security	Accountable
Assist and support the senior management and Information Security Champions Team with their Information Security responsibilities.	Accountable

8. Head of Department

Position: Head of Department	
Reports to – ISSC Committee	
Activities	Level of Involvement (RACI)

Ensure that each employee, within their department, understands and complies with the ISMS Policies and Procedures.	Responsible
Ensure criticality and business risk of their Information Assets and periodically reviewed.	Responsible
Maintain all Information Security related Information Asset Registers, reports and records for their designated department.	Responsible
Determine and review privileges to their Information Assets and Systems.	Responsible
Implement the approved ISMS Policies and Procedure, controls and measures to mitigate risks to the acceptable levels within their areas.	Responsible
Ensure periodic security testing of Information Systems, conduct Internal Assessment and report on any non-compliance to the information security office.	Responsible
Report Information Security incidents and any evidence of information security compromise or any suspicious activity that could potentially expose, corrupt or destroy information and respond to Information Security incidents as and when relevant	Responsible
Promote department wide support and awareness related to the information security.	Responsible
Information security champions are nominated by Senior Management Team and would perform the duties on behalf of Senior Management of the respective department.	Responsible

9. Internal Audit Team

Position: Internal Audit Team	
Reports to – ISSC Committee	
Activities	Level of Involvement (RACI)
Plan the audit process considering the status and Importance of processes and areas to be audited.	Accountable
Define the audit criteria & audit plan.	Responsible
Define the scope of the audit	Responsible
Conduct the audit.	Responsible
Consider the previous audit reports and audit comments	Responsible

Verify the evidence of complying to KGiS ISMS Policies & Procedures	Responsible
Compile the report with findings / observations against the respective controls	Responsible
Provide audit reports to the management.	Responsible

10. Security Incident Response Team

Position: Security Incident Response Team (The Information Security champions team shall also play the role of the Security Incident Response Team)	
Reports to – ISSC Committee	
Activities	Level of Involvement (RACI)
Report Information Security Incidents	Responsible
Conduct 'Root Cause Analysis (RCA)' and initiate immediate containment action.	Responsible
Identify and implement corrective action plan depending on the nature of the incident, point of origin, affected resources and impact	Responsible
Keep the information security office and ICT informed of the status of all the Information security incidents and the actions taken.	Responsible
Maintain Incident Management Forms, updated Incident Logs and protect all evidences collected during the enquiry, in conformance with the relevant rules of evidence (if any) as laid down by the law and applicable to the relevant court of law in which the evidence is to be presented	Responsible

11. Information Security Champions

KGiS shall assign responsibilities pertaining to the coordination of Information Security activities to certain employees acting as Information Security representatives /coordinators across all departments. The duties and responsibilities are to:

Position: Information Security champions
Reports to – Head of Department

Activities	Level of Involvement (RACI)
Ensure adherence to ISMS Policies & Procedures	Responsible
Report any information security breaches or incidents to their direct management	Responsible
Take part in information security awareness trainings & programs	Responsible
Ensure as a focal point for all Information security activities within the department	Responsible

12. Employees

Position: Employees	
Reports to – Line Managers	
Activities	Level of Involvement (RACI)
Employees are responsible for adherence to Information security policies.	Responsible
Notifying all information security issues to the Information Security (IS) officer	Responsible
Ensuring the use of KGiS's asset resources in an ethical and legal manner.	Responsible
Safeguarding all sensitive and confidential information	Responsible
Taking reasonable precautions to prevent unauthorized access to their (end user's) machine and their data by others.	Responsible
Employees and non-employees of KGiS shall not attempt to by-pass or sabotage any of the Company's information security controls.	Responsible
Complying with any other relevant guidance and policies enforced by the concerned authority	Responsible
Complying with other legal and statutory requirements enforced by the authority.	Responsible