CONTENT

This General Instruction applies to all Saudi Aramco organizations. Saudi Aramco's affiliates and subsidiary companies are each responsible for managing their own information security program within their respective organizations.

This General Instruction documents the Saudi Aramco Information Security Analyst (ISA) appointment requirements and documents the ISA Program main stakeholders' functional responsibilities. The ISA Program in Saudi Aramco is monitored by Corporate Security Services Division (CSSD) in coordination with Information Protection Department (IPD), any ISA functional roles referenced in any Saudi Aramco policies, procedures and guidelines must be reviewed and approved by CSSD.

Corporate Security Services Division (CSSD) is the proponent of this GI. All comments and questions related to this GI should be directed to CSSD. Any change to this general instruction will require Safety & Industrial Security (S&IS) Admin Area Head approval and Information Technology (IT) Admin Area Head concurrence.

TABLE OF CONTENTS

*DEFINITIONS OF TERMS

AISA:	Assistant Information Security Analyst
CSSD:	Corporate Security Services Division
CISO:	Chief Information Security Officer
DPP IH:	Data Protection Program Implementation Handbook
ECP&TD:	EXPEC Computing Planning & Technical Division
INT-7:	Data Protection and Retention Policy
IPM:	Information Protection Manual
IPD:	Information Protection Department
IP SAG:	Information Protection Standards and Guidelines
ISA:	Information Security Analyst
ISAD:	Information Systems Audits Division
ISD:	Information Security Department
S&IS:	Safety & Industrial Security

Organization: Saudi Aramco organization that reports directly to a General Management level or above that generates, acquires or store data on behalf of the company.

Information Asset: Any information, information container, or information processing/storage site that is valuable to the organization in terms of criticality and sensitivity, and needs to be protected for its confidentiality, integrity and availability. Any information related to the business or hardware (physical or storage) that has valuable information to the organization.

Information Security Organizations: S&IS, ISD, IPD, CSSD, ECP&TD, and ISAD.

Information Security Policy: Saudi Aramco Corporate Information Security Policies, General Instructions (G.I.s), Standards and Guidelines, and Procedures relating to information protection.

* 1. INTRODUCTION

Saudi Aramco's dependence on information technology to support business functions introduces new challenges and responsibilities. Information Security Analysts (ISAs) are Saudi Aramco's first line of defense and it is vital for them to understand all information security aspects of their organization's information assets and secure them. ISA function is of critical importance for information security within each organization. Organizational information assets access must be controlled only by the designated and approved ISA(s)/AISA(s) supporting that organization.

Saudi Aramco's information security policy requires each organization to design, implement and enforce controls to properly safeguard company information assets and resources within their custody as specified in the Data Protection and Retention Policy (INT-7). Minimum of one ISA must be designated to handle all information security related roles and activities on behalf of the organization head. Additional information security staff (ISA/AISA) should be appointed to support the organization due to special conditions that generate additional workload. The delegation of any information security related roles/activities to other than the approved (ISA/AISA) is prohibited.

2. APPOINTMENT REQUIREMENTS

* Only regular employees, which means permanent Saudi Aramco employees which excludes contractors, consultants, or employees of a Saudi Aramco subsidiary companies or affiliate, can be appointed to act as the respective organization's ISA(s) or AISA(s).

2.1 **Information Security Analyst (ISA) (IV/III/II/I) Job:**

* 2.1.1 **Qualification Assessment:** The appointee should pass the required qualification assessment developed for this specific job.

* 2.1.2 **Assessment/Technical Interview:** The appointee must pass the Assessment/Technical interview conducted by CSSD, in coordination with the proponent organization, as part of the assigning/recruiting process for this specific job ladder.

2.1.3 **Background Investigation (BI):** The appointee must pass the internal Background Investigation (BI) conducted by CSSD.

* 2.1.4 **Job Description Requirements**: The appointee must obtain the minimum requirements per the job description.

* 2.2 **Assistant ISA (AISA) Role:**

Proponent organization may require additional part-time employee to be authorized with the Assistant ISA (AISA) role to support and assist their organization's ISA, based on special conditions that generate additional workload.

The employee that need to be authorized as AISA must meet the following requirements:

* 2.2.1 **Grade Code:** Minimum grade code is 9.

* 2.2.2 **Service:** Minimum of six (6) months with Saudi Aramco to ensure that the employee recognizes the organization business function and is familiar with applications, databases and data communications facilities used to process Saudi Aramco organizational data.

* 2.2.3 **Background Investigation (BI):** The appointee must pass the internal Background Investigation (BI) conducted by CSSD.

3. PROGRAM STAKEHOLDERS' RESPONSIBILITIES

Each stakeholder has specific areas of responsibilities based on supported functions, in relation to this Program as listed below:

3.1 CSSD:

3.1.1 Administer the ISA Program company-wide.

* 3.1.2 Provides the organizations with recommendation, where applicable, in creating a group of ISAs under the Admin Area/General Management level (Centralized or Decentralized Model) to handle related ISA functions for multiple organizations within the concerned level.

3.1.3 Review and approve (permanent/temporary) e-8000 assignment actions for the ISA job.

** 3.1.4 Review and approve appointments to the Assistant ISA role.

* 3.1.5 Conducts an internal Background Investigation (BI) on the designated employees for the ISA job and on the nominated employees for the AISA role. This will be done by conducting due diligence on the nominated employee to mitigate the risk of assigning employees has previously been involved in misconduct in/or outside the company.

* 3.1.6 Conduct periodic/ad-hoc background investigation (BI) of existing ISAs & AISAs, to identify any post appointment convictions or misconduct activities that disqualify them from keeping the ISA job / AISA role.

* 3.1.7 Execute a qualification review of the nominated employee, prior to conducting the ISA job Assessment/Technical Interview.

* 3.1.8 Conduct the Assessment/Technical Interview, in coordination with the proponent organization, for each nominated employee to the ISA job, to evaluate his/her technical, interpersonal and communication skills.

* 3.1.9 Provides the organization head of the ISA job nominee(s) the outcomes of the BI and the assessment interview. The nominee will be classified according to the outcomes, as follows:

* 3.1.9.1 **Eligible**: No derogatory information was found or the information was of a minor nature and should not impact the appointment decision.

* 3.1.9.2 **Not Recommended**: Significant derogatory information was discovered that should be considered by the nominated organization. CSSD will not approve the nominee without a specific approval from proponent organization head.

* 3.1.9.3 **Rejected**: This employee poses a specific security risk or his/her file contains significant derogatory information that, in the professional opinion of CSSD, makes the individual a significant risk. CSSD will not approve the nominee to hold the ISA job.

* 3.1.10 Develop required ISA/AISA information security training strategy, delivery plans and training requirements related to each ISA job grade in coordination with IPD. Coordinate the delivery of any ISA/AISA training courses, conferences or workshops in coordination with IPD & TTSD.

3.1.11 Review and concur any ISA/AISA functional roles if referenced in other corporate policies, procedures or guidelines.

* 3.1.12 Suspend or revoke authorization of any ISA/AISA due to any legitimate cause.

* 3.1.13 Upon request, with consultation with OCD, assist and provide consultations to organization in regard to their ISA/AISA manpower desired.

3.2 IPD

3.2.1 Define technical process, standards and procedures related to ISA's functions.

* 3.2.2 Review and concur new responsibilities to the ISA role, in coordination with CSSD and ISD, where such changes are necessary to improve the information security environment.

* 3.2.3 Provide needed support and consultation using available tools to help ISAs and AISAs to implement and manage their organization's Data Protection Program (DPP).

* 3.2.4 Provide CSSD with available information security monitoring information (e.g. ISA Dashboard) related to any Proponent Organization that can be used to assess effectiveness of their ISA role and activities.

* 3.2.5 Review and concur ISA/AISA information security training strategy, delivery plans and training requirements related to each ISA job grade in coordination with CSSD.

3.2.6 Provide technical input for developing and maintaining training material related to ISA/AISA courses.

3.3 Organization Head:

* 3.3.1 Appoint a minimum of one (1) employee to fill the designated ISA job position in accordance with the following options:

* 3.3.1.1 An appropriately qualified employee is assigned as the organization's permanent ISA.

* 3.3.1.2 A capable employee is assigned as the organization's ISA on a temporary assignment base, due to the shortage of qualified employee(s) to be appointed as permanent ISA or due to the absence of the permanent ISA(s) for any reason.

* 3.3.1.3 Implement the recommendation(s) as detailed in Section 3.1.2 of this GI.

* 3.3.2 Appoint a minimum of one employee to fill the designated ISA job position or ensure that qualified ISA(s) supporting the respective organization for a temporary period, or when recommendation in 3.1.2 is implemented.

* 3.3.3 Approve and delegate authority to the appointed ISA(s) and AISA(s) for controlling access to any applicable support systems/applications (e.g., SAP, Microsoft, Oracle, Active Directory, Sharek, e-Cabinet, ECC, Plant Control, IT Managed Servers, Intelligent-Field, etc.) belongs to their organization.

* 3.3.4 Ensure that additional information security staff (ISA/AISA) are appointed to support the organization additional workload, magnitude of organization's manpower or geographical locations.

* 3.3.5 Ensure that the appointee is a trustworthy employee and model the company's business ethics.

* 3.3.6 Ensure that both the organization ISA(s) and AISA(s) implement, comply with, and enforce the company's Information Security Policy.

* 3.3.7 Ensure that appropriate PMP goals are assigned to both the ISA and AISA — by their respective superiors — to perform the duties stated in this GI.

* 3.3.8 Ensure that ISAs undertake appropriate technical training courses as recommended by CSSD & IPD.

3.4 ISA:

3.4.1 **Organizing and Coordinating the Data Protection Program:** Provide technical advice, guidance and assistance to organization management, to identify and document business information security needs, objectives and procedures, to ensure the protection of business information, while ensuring compliance with information security policies. Develop and maintain the organization's Data Protection Manual, policies, procedures and standards, based on knowledge of best practices and compliance requirements, and ensure the acceptance of these across the organization.

3.4.2 **Information Asset Management:** Coordinate and collaborate to generate inventory of information assets for the organization, and ensure that the organization data is classified and maintained as per GI 710.002. Also conduct periodic review of published contents as cited in GI 850.011.

3.4.3 **Risk Assessment & Risk Treatment:** Lead the process of risk management to safeguard business data as per INT-7 through risk assessment and risk treatment activities.

3.4.4 **Access Control:** Maintain access control to information/computing assets and resources as per GI-710.002, and review access rights on a regular basis, and revoke or adjust, as per the changing business needs.

3.4.5 **Data Protection Awareness:** Ensure that appropriate awareness techniques for the awareness program are selected, and perform several awareness activities for his/her organization during the operational year.

3.4.6 **Reporting Information Security Observations:** Prevent and detect incidents, and make security observations, by promoting computer security awareness among users and encouraging them to report any computer or system misuse, security breach or other irregularity.

3.4.7 **Data Backup and Retention:** Create awareness among the staff about backup and retention. Coordinate to identify and document the data backup needs and data retention period as per business and regulatory requirements.

3.4.8 **Business Continuity Planning:** Coordinate business continuity requirements for his/her respective organization with the Business Continuity Division of IPD, to comply with the approved corporate business continuity requirements.

3.4.9 **Physical Security:** Enforce the guidelines for physical security in the organization to secure information processing/storage sites (such as the control room, archive room, library, etc.) and information processing/storage hardware, from physical and environmental threats, as per GI-710.002.

3.4.10 **External Party Security:** Ensure that guidelines and best practices of data protection are considered and enforced when dealing with external parties.

3.4.11 **Software Management:** Ensure that data protection controls are applied as appropriate for non-IT managed software.

3.4.12 **Data Protection Reviews:** Perform regular internal data protection reviews to assess the completeness and compliance of the critical functions and controls implemented, as part of the Data Protection Program, such as information asset management, risk assessment and risk treatment.

3.4.13 **Compliance Management:** Develop and implement a comprehensive Data Protection Internal Compliance Program, in conjunction with the organization's management.

3.4.14 **Corrective and Preventive Actions:** Ensure that proper corrective and preventive actions are executed on a timely basis, to ensure proper resolution of the identified information protection (IP) observations.

3.4.15 **Data Protection Performance Reporting:** Provide management the insight to implementation, adequacy and effectiveness of the Data Protection Program.

3.4.16 **IT Assets Management:** Perform organizations' IT assets management and inventory controls, as cited in GI 299.110.

3.4.17 **Data Protection Program Implementation Handbook:** Perform any assigned functional roles identified in the **DPP IH** .

3.5 **AISA Role:**

Assistant ISA role is a part-time supporting role that will be achieved in coordination with the respective organization's ISA to fulfill information security requirements under the following conditions:

3.5.1 Managing and implementing the Data Protection Program.

3.5.2 Covering geographically distributed work locations.

3.5.3 Controlling access for specific IT systems or internally developed applications (e.g. SAP, ITAMS, ShareK, e-Cabinet, etc…).

3.5.4 Supporting complex IT projects that generate additional workload.

* 4. AFFILIATES AND SUBSIDIARIES OF SAUDI ARAMCO

Saudi Aramco's affiliates and subsidiary companies are each responsible for their information security within their respective organizations. A Saudi Aramco employee may assist in the provision of those services, only if Saudi Aramco agrees to provide such services pursuant to a service agreement between Saudi Aramco and the relevant affiliate or subsidiary companies and without violating the existing Saudi Aramco corporate separateness policies.

* 5. WAIVER:

Exception or waiver to certain ISA/AISA appointment requirements will require an official request to CSSD Administrator from the concerned organization Management or above. Permanent ISA will require also the Personnel

Department approval. Such waivers are for circumstances when suitable nominees are unavailable, or until adequate training and development of a dedicated nominee get completed.

6. SIGNATORY

Recommended: ____________________ Date: ________________
Khalid A. Buali (A)
Administrator
Corporate Security Services Division

Reviewed: ____________________ Date: ________________
Khalid S. Al-Harbi (A)
Manager
Information Protection Department

Concurred: ____________________ Date: ________________
Yousef A. Al-Ulyan,
Executive Director
Information Technology

Date:

Approved: ____________________ ________________
Bader F. Al-Qadran
Executive Director
Safety & Industrial Security

Appendix A
ISA support related General Instructions (GIs)

GI No.	Description	Proponent
0299 080	General Business Computing Product Approval, Funding, and Categories	IT/Area IT Department
0299 110	Computer Asset Management System	IT/Area IT Department
0299 120	Sanitization and Disposal of Saudi Aramco Electronic Storage Devices and Obsolete/Unneeded Software	IT/ Information Protection Department
0299 220	Remote Access to Saudi Aramco Computer Systems and Networks	IT/ Information Protection Department
0299 223	Saudi Aramco Information Protection Management	IT/ Information Security Department
0299 225	Information Security Acceptable Use Policy	IT/ Information Security Department
0299 226	Enterprise Cybersecurity Policy	IT/ Information Security Department
0299 227	Cybersecurity Consequence Management	IT/ Information Security Department
0710 001	Saudi Aramco Identification Cards	S&IS/Industrial Security Support Department
0710 002	Classification and Handling of Sensitive Information	S&IS/Industrial Security Support Department
0850 011	Review and Approval of Saudi Aramco Intranet Web Content and Social Media Use	Public Relations Department

These GIs are available in the http://sharek.aramco.com.sa/cops/GI/Pages/home.aspx website.

Appendix B
Information Protection Manual (IPM)

IPM consists of specific Information Protection Standards and Guidelines (IPSAG) that outline the requirements for security and operational support standards and guidelines. The intranet website http://sharek.aramco.com.sa/orgs/30020119/30011804/Pages/IP_Policies.aspx lists the current IP Manual.