CONTENT

This General Instruction (GI) outlines the organization and management of Information Protection within Saudi Aramco to ensure an effective implementation of controls and practices to protect Saudi Aramco electronic data, network and computing resources. Information Protection means the protection of electronic data, network and computing resources from unauthorized access, use, disclosure, disruption, modification or destruction.

The content of this GI includes:

1. Purpose
2. GI Proponent
3. Information Protection
4. Responsibilities
5. Related Documentations

1. PURPOSE

The purpose of this General Instruction is to ensure the efficient and streamlined implementation and operation of Information Protection within Saudi Aramco. It also establishes the authorities and responsibilities for Information Protection within Saudi Aramco. Saudi Aramco affiliates and subsidiary companies are excluded from the scope of this GI.

2. GI PROPONENT

Information Protection & Technology Planning Department (IP&TPD) is the proponent of this GI. Further inquiries should be addressed to IP&TPD.

3. INFORMATION PROTECTION

The Saudi Aramco Information Protection includes the Saudi Aramco Information protection policies and standards, supporting processes and the activities performed to support the protection of Saudi Aramco corporate information systems and assets in support of the corporate data protection and retention policy (INT-7).

4. RESPONSIBILITIES

4.1. Steering Committee

The Steering Committee consists of Business Line representatives, nominated or delegated with authority to represent the Head of each business line, and representatives of the Information Protection organizations. Information Protection Organizations are those organizations assigned by company management to support Information Protection. The Steering Committee recommends general Information Protection directions and initiatives within Saudi Aramco. It also serves as a forum where major information protection issues can be presented along with proposals and resolutions. The Steering Committee also directs the implementation or evaluation of specific recommendations to the

appropriate Business Line. The Information Protection & Technology Planning Department is responsible to arrange the Steering Committee meetings and record the meetings

4.2. Information Protection & Technology Planning Department

The Information Protection & Technology Planning Department manages and coordinates the Saudi Aramco Information Protection Program under the authority of IT Executive Management for systems connected to the Saudi Aramco network. These include developing and maintaining the Information Protection Roadmap (Technologies, tools, programs and services to enhance and implement Information Protection), developing and managing Information Protection policies and Information Protection Standards & Guidelines, coordinating or conducting IT risk assessments, compliance assessment/monitoring or checks, corporate information incident management and awareness as required.

4.3. Data Proponents

Data proponents (as defined in GI-710.002) will bear full authority and responsibility for classifying; controlling access to; and safeguarding of the data during its retention period, for the benefit of the Corporation as a whole. Proponents are also responsible for advising data classification to the custodians of the data. For more information see INT-7.

4.4. Computer Security Administration (CSA)

The Computer Security Administration (CSA) conducts investigations and forensic examinations involving serious cases of computer misuse, information disclosure, or matters where computer resources are used to subvert or damage Saudi Aramco resources or other assets. CSA also manages and oversees the Computer Security Liaisons (CSLs) program.

4.4.1 Computer Security Liaisons (CSLs)

The Computer Security Liaisons (CSLs) are appointed by their respective department heads to implement, and enforce controls for information/computing assets and resources within their custody. They are also the local point of contact for their Departments' information security related activities. The CSL's main responsibilities are listed in the CSL Standard & Guidelines (**CSL SAG-002).**

4.5. Access Control Groups

The Access Control Groups are responsible to implement Corporate Computer Security requirements by administering logical access control for users and systems under their control. They also provide incident response capabilities within their respective Data Centers.

4.6. Internal Auditing Department

Internal Auditing is an independent appraisal function within the Company. It examines and evaluates the adequacy and effectiveness of the overall system of controls adopted by Management to enhance the achievement of established objectives and goals. As such Internal Auditing also examines and

evaluates the controls on Saudi Aramco computing resources. (See Policy Statement Internal Auditing for more information)

4.7. Users

Users are responsible to take the necessary due care to protect company information and resources under their control, custody or use. They must also comply with Company information protection policies and report suspected unauthorized use of their user IDs or suspicious activity to their Computer Security Liaison(s) (CSL).

5. RELATED DOCUMENTATIONS

The following documentations are also applicable to Information Protection within Saudi Aramco:

- Data Protection and Retention Policy (INT-7)
- Information Protection General Instructions
- Information Protection Manual
- Process Automation Networks & Systems Security (SAEP-99)
- Process Automation Networks Connectivity (SAES-Z-010)
- Saudi Aramco Computer Use Policy (SA-9595)
- Saudi Aramco Computer Use Agreement (Non-Employee) (SA-9696)

Recommend:

_____
Manager, Information Protection & Technology Planning Department

Concur:

_____
Executive Director, Information Technology

Concur:

_____
General Manager, EXPEC Computer Center

Concur:

_____
Executive Director, Safety and Industrial Security

Concur:

_____
LAW Department

Concur:

_____
Sr. Vice President, Operations Services

Approve:

_____
President and Chief Executive Officer