CONTENT:

***** This instruction standardizes the procedure for classifying and reclassifying Company information according to its sensitivity and defines the requirements for labeling, storage, disclosure, distribution and destruction of sensitive information. It also identifies the responsibilities of Company employees and contractor personnel performing services for Company organizations, who deal with confidential and other sensitive information. It includes the following sections:

1.0 GI PROPONENT

Except as otherwise stated herein, Industrial Security Planning & Support Services Department (ISP&SSD) is the proponent of this GI. Further inquiries should be addressed to ISP&SSD Manager, Box 90, Dhahran. Any exception or changes to the procedures in this instruction will require ISO General Manager's approval.

* 2.0 DEFINITIONS AND ABBREVIATIONS

2.1 DEFINITIONS

* 2.1.1 **Company information and data**: Information and data related to the operations and activities of the Company and its employees, regardless of the form or media in which the information is recorded or maintained – examples include, but are not limited to memoranda, letters, correspondence, e-mails, reports, maps, drawings, photographs, videos and audio tapes, electronic and computer files, e-documents, computer applications, and material placed or stored on the World Wide Web (www), Intranet/Extranet pages, databases, microfilm, and microfiche, etc.

2.1.2 **Proponent organization** – A "proponent" is the department within the Company that creates, compiles, or maintains such information and data, or receives such information and data from third parties.

** 2.1.3 **User organization** – A "user" is the department within the Company that uses the information created or compiled by the proponent organization.

* 2.1.4 **Sensitive information and data**: Information and data which could have a negative impact on the operations, activities, finances, image, reputation, or competitive advantages of the Company or could harm or damage either the Company, its employees, or its shareholders if released to the public. Because of its nature, content, or subject matter, sensitive information and data must be maintained and protected by the Company and not released to the public without appropriate authorization from management. Sensitive information and data can be classified as "Restricted," "Confidential" or "Government Confidential" and may only be accessed, disclosed, or distributed to authorized individual users, or organizations pursuant to appropriate levels of authorization as set forth herein.

** 2.1.5 **Physical Security Protection**: The operational and physical safeguards put in place to control access to sensitive information and data and to protect against threats, reduce vulnerabilities, limit the impact of an improper or inadvertent disclosure, and protect against damage to the information, data and company assets and personnel.

** 2.1.6 **Risk Assessment Strategies**: The identification of potential hazards, the assessment of damages which would be incurred, and the evaluation of the probability of occurrence of potential hazards which are used as criteria to determine the level of Physical Security Protection needed to appropriately safeguard Company information and data.

** 2.17 **Intellectual Property**: Information or intangible property that has been created by the human mind or intellect in such a manner that it has value and is subject to protection by copyright, patent, trademark or as trade secrets. The Company's intellectual property includes inventions, know-how, software, data, written material symbols and other such property that is owned by the Company.

* 2.2 **ABBREVIATIONS**

AISOD	:	Area Industrial Security Operations Department
CSS	:	Corporate Security Services
CCCD	:	Customer Care Center Department
COD	:	Computer Operations Department
CA	:	Computer Applications
ES	:	Engineering Services
ISP&SSD	:	Industrial Security Planning & Support Services Department
IPD	:	Information Protection Division
IT	:	Information Technology
ISO	:	Industrial Security Operations
MSP	:	Medical Services Policies
OSD	:	Office Services Department
PRD	:	Public Relations Department
HRP&PD	:	Human Resources Policy & Planning Department
S&IS	:	Safety & Industrial Security
SAA	:	Saudi Aramco Affairs
SAMSO	:	Saudi Aramco Medical Services Organization

3.0 CORPORATE POLICIES AND ASSOCIATED REQUIREMENTS

3.1 **Policy No. INT-7** (Data Protection & Retention) states that "Proponent organizations generating, acquiring or storing data on behalf of the Company 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. Users of the data, including the proponent organization, will bear full responsibility for the provision of appropriate data security while they are using the data. Computer organizations and custodians of computers, which process/store sensitive, or valuable data are responsible for providing the necessary access control software; backup; disaster recovery/execution; and protection within their areas of responsibilities."

** 3.2 **Policy No. INT-9** (Intellectual Property) states that "Intellectual Property" shall be acquired, developed, protected, used and exploited in a manner that will maintain its confidentiality and maximize the Company's profit from its use and exploitation. Intellectual property shall be managed in the same manner as other valuable Company assets, i.e., identified with asset number, value, custodianship, etc.

3.3 To comply with Policy No. INT-7, sensitive information and data shall be classified/reclassified with its retention period and properly safeguarded. Users must not upload, download, publish, transmit or otherwise disclose sensitive information or data concerning the Company and its operation and activities on or through the Internet or any other transmitting media without prior approval of authorized Company Management. The sensitive information, data and intellectual property conveyed or shared using World Wide Web (WWW) pages, Systems, Applications, and Products (SAP) modules, database applications, Intranet/Extranet, e-Commerce, e-Business, Business to Business and similar applications must also be classified, reclassified and protected according to its classification.

** 3.4 To comply with Policy INT-9, researchers and technical workers at Saudi Aramco will be required to maintain a laboratory or process notebook for record keeping of intellectual property and patent protection. Such a notebook should provide a complete record of research or innovative work that could be understood and repeated by qualified personnel. The notebook is also a place for recording any planned work or new ideas, to complement the innovation Web site idea section. Proponent or user organizations may contact Intellectual Assets Management (IAM) group concerning the measures designed to protect against premature publication or release of information relating to Saudi Aramco Intellectual Property.

4.0 CLASSIFICATION CATEGORIES

* Proponent organizations are responsible for classifying information into one of the following five categories (the last three are sensitive). In case of uncertainty or disagreement as to the proper classification of information, ISP&SSD, Law Department or IPD, as appropriate, will be consulted in determining its proper classification or reclassification. PRD will be consulted to review the structures, presentations and appearance of content to be placed in Web pages, systems, modules, applications, etc. Refer to the appropriate general instructions such as 299.210 (Saudi Aramco Internet Use), 850.003 (Corporate Identity Guidelines), 850.006 (Review and Approval of Saudi Aramco Publications & Articles) & 850.011 (Review and Approval of Saudi Aramco Intranet Web Content and Web Sites) for more details.

* 4.1 **Public information** is information intended for general distribution inside and outside the Company. This information can be made public without any negative consequences for the Company. The release of this information has no potential for negatively impacting Saudi Aramco operations or its employees. The integrity of this information is important but not vital. Proponent organizations shall ensure that the information being provided is accurate, complies with Corporate Identity guidelines, and meets Company standards. However, Company responses to requests from third party organizations and other entities shall be specific, accurate and concise. For preparation of written responses, proponents shall coordinate with PRD. See section 7.1 for classification criteria, examples and storage/destruction guidelines.

* 4.2 **Company General Use information** is information that may be distributed outside the Company with prior approval of the proponent Department Manager and is considered appropriate for general distribution to company or contractor employees within the Company. This information is accessible to Company employees, consultants and contractor employees performing services for Company organizations on a need-to-know basis to satisfy the Company's business requirements. The disclosure of this information outside of the Company has no potential for negatively impacting Saudi Aramco operations or its employees. Data integrity is important but not vital. See section 7.2 for classification criteria, examples and storage/destruction guidelines.

* 4.3 **Restricted information** is information which, if accessed by unauthorized persons, could negatively impact the Company's operational effectiveness, result in financial loss, provide improper advantage to a competitor or contractor, or seriously impact customer confidence, the Company's business reputation and/or image. Access and usage is limited to authorized Company employees, consultants and contractors performing services for Company organizations on a need-to-know basis to satisfy Company business requirements. All reasonable steps will be taken to prevent disclosure of this information to unauthorized persons. Data integrity is vital. All Company information not published for public or Company General Use is considered "Restricted" unless given a higher classification (i.e., "Confidential" or "Government Confidential"). Department managers and above may delegate the authority to employees to grant access to "Restricted Information" when necessitated by operational requirements. Release or disclosure of such information within and outside the Company may be allowed with prior approval from the proponent Department Manager. See section 7.3 for classification criteria, examples and storage/destruction guidelines.

* **Note:** "Historical" and "vital" information as defined in Information Management Guidelines shall be classified as "Restricted", with its associated retention requirements unless given a higher classification (i.e., "Confidential" or "Government Confidential"). See the Saudi Aramco Records Manual for the definition and further information.

* 4.4 **Confidential information** is information which, if accessed by unauthorized persons, could seriously impact the Company's operational effectiveness, results in a serious financial loss, provide significant, improper advantage to a competitor or contractor or damage confidence and/or the Company's business reputation in a serious manner. Confidential information (hardcopy or electronic) is only accessible to a limited number of Company employees on a need-to-know basis. Such information should be designated as "Confidential" by concerned Saudi Aramco management or their designee. Data integrity is vital. Release of "Confidential information" within the Company

requires the approval of the proponent Department Manager or higher. See section 7.4 for classification criteria, examples and storage/destruction guidelines.

For security related issues, release of confidential information to Government security agencies or other government agencies requires the approval of the Executive Director – Safety & Industrial Security or his designee. Release of non-security related confidential information to Government agencies must be through the SAA Vice President or his designee. Release to contractors or other non-governmental third parties requires the approval of the proponent organization's executive management or their designee.

* 4.5 **Government Confidential information** is information which has been identified by Saudi Aramco Affairs, Industrial Security (for security oriented information) or other Company organizations, as important to the vital interests or security of the Kingdom and which requires special attention to prevent unauthorized disclosure. This information is considered extremely sensitive and is designated "Government Confidential" by the SAA Vice President or S&IS Executive Director in consultation with the proponent organization and Law Department, where appropriate. Such information is only accessible to selected employees of a department on a need-to-know basis. The classification, reclassification, release, or disclosure of such information by any organization other than Saudi Aramco Affairs or Safety & Industrial Security requires the approval of the proponent organization's executive management and should be coordinated with Saudi Aramco Affairs or Industrial Security and Law Department. Exchanges of sensitive information with Government agencies by Corporate Planning are also authorized in coordination with Saudi Aramco Affairs. See section 7.5 for classification criteria, examples and storage/destruction guidelines.

** 4.6 In the event two types of sensitive information or data (e.g., restricted information and government confidential) are combined in a hardcopy format or electronic document, the applicable information will be reclassified or maintained in accordance with the stricter classification level.

5.0 GENERAL REQUIREMENTS

* 5.1 Proponent organizations, with the assistance of the supporting computer organizations, are responsible for identifying sensitive information or data and assigning it the appropriate classification in accordance with corporate policies (INT-7 & INT-9) and this GI. Proponent organizations are required to implement the security measures that will be applied to protect information maintained in Web applications, computer systems, personal computers and all other electronic systems and devices, especially when it is carried by employees outside Company premises. The Information Protection Division should be consulted for the current corporate security measures to protect information maintained in electronic format. Proponent organizations are also responsible for maintaining appropriate access controls provided to users who are physically accessing computer or data centers. ISP&SSD and/or AISOD reviews and endorses all security measures used for physical access control protocols to computer or data centers and to protect hardcopy information (i.e. information that is not in electronic format). IPD reviews and approves the security measures used to protect information maintained in electronic format.

* 5.2 Proponent organizations (owner of the information or electronic documents) are responsible in setting the classification or reclassification criteria of sensitive information to a stricter or lower level, with its associated retention requirements in accordance with this G.I. In addition, the proponent organization must specify the retention period of information at the time of classification or reclassification before it is stored or uploaded in any computer system or application and periodically review those requirements. When the specified retention period of previously classified information has elapsed, the information shall be scheduled for reclassification and then may be destroyed as defined in Section 7.0.

* 5.3 As provided herein, "Confidential" information and "Government Confidential" information is to be labeled as such. "Restricted" information may or may not be labeled at the discretion of the proponent Department Manager. All sensitive information must be treated according to its classification in accordance with this GI. The sensitive information must be treated appropriately whether previously labeled or not.

5.4 When the information is of a legally sensitive nature, Law Department must clear its release. Examples include, information concerning Company operations whose disclosure must be authorized by the Government, legal opinions or analyses authored by members of the Law Department or outside counsel, material subject to production in response to legal process, material subject to a legally recognized privilege (marked "Privileged and Confidential", "Confidential: Attorney Work Product" and the like). See Section 7.4 for classification criteria, examples and storage/destruction guidelines.

* 5.5 Information transmitted using the Internet, wireless applications and other electronic media is at high risk of disclosure, modification, or loss. The sensitive information should be encrypted during transmission unless the transmission is on a dedicated wire or an isolated network segment where sniffing or capturing network traffic is not possible. The encryption, which is a tool to be utilized so that information cannot be intercepted or read by unauthorized individuals, must be strong enough so that it should not be cracked or compromised. See the Information Protection Manual for more information on encryption standards. Users must not exchange, transmit, post or publish any sensitive information that may compromise the security of Saudi Aramco, its personnel or property or the privacy rights of individual employees or third parties (where the Company has a legal or contractual obligation to protect such privacy).

* 5.6 Users must not share, write down, electronically store (without strong encryption), or otherwise disclose the password or employ any methods that defeat the Company's individual identification and authorization technologies. For more information concerning data protection, refer to the Information Protection Manual.

* 5.7 For information concerning the protection of data on a portable personal computer or microcomputer, refer to the Information Protection Manual.

* 5.8 Information produced inside the Company and intended for publication outside the author's department, including the posting of information on Web pages and/or sites, must be reviewed and approved by the Public Relations Department, according to the criteria and procedures set out in the following GIs; 850.003 (Corporate Identity Guidelines), 850.006 (Review and Approval of Saudi Aramco Publications & Articles), and 850.011 (Review and Approval of Saudi Aramco Web Content) and 431.001 (Protection of Intellectual Property). PRD is responsible for the review and approval of this information before its release.

5.9 This GI does not authorize the dissemination of information in violation of any agreement between the Company and any third party with respect to the handling or dissemination of information of any sort.

* 5.10 Many documents labeled prior to the year 1995, which is the original issue date of this GI will fall into the "Public", "General Use," "Restricted", "Confidential" or "Government Confidential" categories. This GI does not require documents previously labeled "Confidential" or "Government Confidential" to be relabeled to reflect the new or re-classification until the documents are updated for some other reason. However, all new and updated documents shall be classified according to the categories in this GI.

5.11 As per Company Policy INT-7, technical and other confidential business information reflecting past operations, existing conditions or proposed actions will only be disclosed to third parties on a need-to-know basis or as required by law, and with proper Management, and if necessary, Governmental authorization.

** 5.12 As per Company Policy INT-9, Intellectual Property which is of a technical and sensitive nature should also be reviewed by Intellectual Assets Management Group of the Engineering Services Organization to ensure that it contains no subject matter which has value to the Company and therefore should first be protected before being placed into the public domain and potentially destroying the Company's ownership interest (i.e., such as a patent).

* 5.13 Employees, consultants and contractor personnel performing services for Saudi Aramco organizations are expected to exercise caution and good judgment in discussing sensitive Company information with others, so that sensitive information is not released to third parties or unnecessarily disseminated within the Company. Also, employees and contractor personnel shall ensure that information discussed with outsiders does not compromise Saudi Aramco's reputation, security operations, technology or long term strategies.

* 5.14 ISP&SSD, IPD, Law Department or PRD, as appropriate, must review any deviations from this GI on request from any organization. After the requested deviation is documented, reviewed and approved by ISP&SSD, IPD, Law Department or PRD, as appropriate, the users and/or proponent organizations (department manager) requesting the deviation must obtain the approval of its General Manager or above and the ISO General Manager or above.

6.0 RESPONSIBILITIES

6.1 Industrial Security Planning & Support Services Department (ISP&SSD) has oversight responsibility to monitor the classification of sensitive information not in electronic format and approval authority with respect to all security measures used to protect hardcopy information (i.e., information that is not in electronic format). ISP&SSD will provide, upon request from proponent organizations, recommendations and standards for the storage/destruction of hardcopy information and its protection. ISP&SSD will also advise and assist departments, upon request, in the

development of internal procedures that include measures for classification of sensitive information, physical access measures to computer/data centers, and guidelines for the protection of hardcopy information.

* 6.2 Information Protection Division has the overall authority for review and approval of methods used to protect information maintained in electronic format. IPD will advise and consult with departments, upon request, in the development of internal procedures, measures and guidelines for the protection of electronic information. IPD is also responsible for updating the Information Protection Manual and its distribution to all Company organizations. This includes notifying all business users through announcements on the use of portable devices, including laptops and protection of company information, which must not be disclosed to unauthorized persons.

* 6.3 Area Industrial Security Operations Department will provide physical security manning at the computer/data centers, in their area of responsibility, upon request from proponent organization. Also, AISOD, in coordination with ISP&SSD, may also assist departments in complying with this GI, including the destruction of hardcopy information. When requested, AISOD may review and endorse departmental security measures used to protect sensitive information in hardcopy format. Upon request from proponent organizations, AISOD shall delegate employees to witness and certify destruction of sensitive information and shall seek assistance from ISP&SSD in the development of security measures related to the sensitive hardcopy information.

6.4 Corporate Security Services will conduct investigations related to serious unauthorized disclosure/distribution, theft, alteration, or loss of both hardcopy and electronic sensitive information where Company interests have been affected. ISP&SSD and IPD will assist CSS in conducting these investigations as required. CSS will also be responsible for witnessing and certifying destruction of obsolete computer devices and other electronic items such as tapes, CDs, hard drives, etc., that contain sensitive data when requested by proponent organizations. A CSS representative should physically participate in the destruction of computer devices and other electronic items that contained sensitive information, (See GI 299.120).

6.5 Company Management (**http://mgtg.aramco.com.sa/toc.asp**) will ensure that sensitive information is identified, properly classified, reclassified and labeled, and may at its discretion change the classification to a higher or lower level for any particular information. Company Management can consult ISP&SSD or IPD, as appropriate, for assistance in the requirements of this GI identifying, classifying, reclassifying and labeling sensitive information. Company Management must authorize the reclassification of sensitive information. Release of sensitive information to outside parties will follow this GI. The proponent organization will resolve any disagreement regarding classification or labeling with Industrial Security, IPD, Law Department, or Saudi Aramco Affairs, as appropriate.

* 6.6 Proponent or user organizations generating, acquiring or storing data on behalf of the Company will bear full authority and responsibility for classifying/reclassifying when information is no longer sensitive, controlling access to and safeguarding of the information and data during its retention period, for the benefit of the Company as a whole. Proponent or user organizations are responsible for:

** 6.6.1 Advising data classification to the custodians of the data or intellectual property protection, (See Policy: INT-7 and INT-9).

** 6.6.2 Ensuring sensitive information in their custody and being used by their employees and contractor personnel is protected.

** 6.6.3 Providing physical security protection and risk assessment strategies with the following:

** 6.6.3.1 For Physical Security protection:

- Access to the system console is adequately restricted with access authorization.
- Key entry systems such as PIN code, swipe card, biometric, etc., are used and alternatively appropriate logs are provided to identify the personnel who entered the secured location.
- Security guards are deployed at the entry points.
- Buildings or offices are properly secured where sensitive information and data are maintained.
- Cameras are installed as appropriate.

** 6.6.3.2 For Risk Assessment strategies:

- Identifying threats that could adversely affect operations and assets of the Company.
- Identifying the value, sensitivity and criticality of the operations and assets that could be affected
- Estimating the potential losses or damages that could occur if a threat materializes, including recovery costs.
- Identifying cost-effective actions to mitigate or reduce the risk.
- Documenting the results and developing an action plan.
- Providing necessary access control software and hardware devices for protection of sensitive information and data maintained through computers (including laptops), data centers, systems and applications.

* 6.7 Supporting Computer Organizations are responsible for assisting proponent organizations, individual users and custodians in developing technical solutions for classification requirements. In addition, computer organizations, users and custodians of computers that process/store sensitive or valuable information are responsible for implementing the necessary access control software, backup system, disaster recovery planning/execution and protection within their areas of responsibility. They will ensure that sensitive information is effectively protected and that appropriate methods are used to destroy this information beyond recognition when no longer needed. ISP&SSD, AISOD or IPD, as appropriate, should be consulted to determine the appropriate means of destroying Company sensitive information and its associated storage/devices.

* 6.8 IT Customer Care Center Department is responsible for the update and implementation of the policies and procedures as stated in the Records Management Manual and the Information Management Guidelines to be consistent with GI. IT CCCD shall also update Saudi Aramco form SA-9546 to be used by all organizations for the purpose of retention requirements and destruction of sensitive information.

* 6.9 Service organizations such as Community Services, Computer Applications, Communication Engineering & Technical Support Department, IT Customer Care Center Department, Computer Operations Department and Office Services Department will provide a secure environment for the processing, transmission, handling and storage of all Company information and data. User departments shall work with these organizations to ensure their storage and protection requirements are met.

** 6.10 Public Relations Department is responsible for reviewing and updating GI 850.011 with applicable changes in policies and procedures and assisting the organizations to adhere to the Company policies while publishing information/contents in Intranet/Extranet and Internet Web sites. PRD is also responsible for reviewing and approving articles for release to the public. See GI 850.006 for more details.

** 6.11 Saudi Aramco Affairs is responsible for assisting the Company organizations to understand the importance of Government Confidential information and preventing its unauthorized release or disclosure in coordination with Corporate Security Services.

** 6.12 Saudi Aramco Medical Services Organization (SAMSO) is responsible for reviewing and updating its administrative policies and procedures contained in MSP-231 and MSP-232, which describe the confidentiality of sensitive medical information. ISP&SSD and IPD can be consulted if needed.

** 6.13 Engineering Services is responsible for reviewing and updating the guidelines and procedures stated in SAEP-120 and 127 related to the drawings of Saudi Aramco vital and restricted facilities. Engineering Services Organization (Intellectual Assets Management Group) is also responsible for updating and distributing guidelines related to the information and issues on Intellectual Property (Policy: INT-9). ISP&SSD or IPD can be consulted if needed.

** 6.14 Personnel Department is responsible for reviewing and updating the conflict of interest and business ethics policies contained in SA-8942 and its implementation.

** 6.15 Human Resources Policy & Planning Department is responsible for updating Industrial Relations Manual regarding the release of personnel information and disclosure procedures in accordance with this GI.

** 6.16 Law Department will provide legal opinions or advice to Company organizations when information of a legally sensitive nature is to be released or disclosed inside or outside the Company or retained for legal reasons (e.g., in anticipation of or use in litigation) beyond its normal retention period. The Law Department shall advise all Company organizations regarding the classification and protection of legally sensitive or confidential information.

** 6.17 Long Range Planning Department is responsible for reviewing and updating data protection and retention policy (INT-7) with possible changes in the regulations and notifying all Company organizations of its implementation.

7.0 CLASSIFICATION, RECLASSIFICATION CRITERIA AND STORAGE/DESTRUCTION GUIDELINES

Subject to the qualifications set forth herein, proponent organizations are responsible for classification/reclassification of information for the benefit of the Company before it is published, transmitted or distributed within or outside the Company. In case of uncertainty or disagreement, ISP&SSD/AISOD, Law Department or IPD, as appropriate, can be consulted in determining the proper classification/reclassification of the information in question. In general, the declassified items, which are marked for destruction, shall be destructed using a shredder or other means. The following criteria and examples can be used to determine the classification of information within Saudi Aramco:

7.1 Public information:

Criteria:

Published material designed for Company-wide and public distribution. Includes documents originating from outside the Company and intended for public consumption.

* **Examples:**

- Newspapers and magazines.
- Vendor published non-proprietary software or equipment manuals.
- General use manuals and reference books.
- Loss Prevention publications intended for public distribution.
- CDs/audio/videos and photographs designed for public use.
- Promotional items.
- Information available on the Company's Internet Web site.

Storage/Destruction Guidelines:

* No special guidelines are defined for storage or destruction, since this information is not sensitive. Departments may establish procedures for the handling and storage of public information according to the operational needs.

7.2 Company General Use information:

Criteria:

- Material designed for distribution to Company and contractor employees that will be used in Company-related business functions.
- Disclosure within the Company for business use is not expected to have a negative impact on Company operations or its employees or third parties.

* **Examples:**

- General Instruction Manuals, Online Industrial Relations Manuals (HR Policies), Contracting and Accounting Manuals, Operating Instruction Manuals, and Departmental Internal Controls.
- General accounting records, general correspondence and departmental training materials.
- Saudi Aramco engineering standards, specifications and procedures.
- Journal entries and voucher information.

- Proposals, reports and analyses internal to business lines, unless classified at a higher level.
- Organization transformation/outsourcing plans, service level agreements, performance measures, etc.

Storage/Destruction Guidelines:

* No special guidelines are defined for storage or destruction, since this information is not sensitive. Departments shall establish procedures for the handling and storage of general use information according to the operational needs.

7.3 **Restricted information:**

Criteria:

- Access and usage are based on job needs and current Company policies.
- Disclosure is expected to negatively impact limited areas of operations.
- Disclosure might adversely affect efficiency of Company operations but not the accomplishment of overall goals or objectives.
- Disclosure typically may affect personal privacy of employees or embarrass the organization involved.
- Disclosure may result in a financial loss or provide improper advantage to a competitor or contractor.
- Primary impact is on personnel and customer confidence.

Examples:

- Employee career planning programs.
- Engineering drawings, unless classified at a higher level.
- Contracting or purchasing plans, active or historical contracting or purchasing data, unless classified at a higher level.
- Engineering Services - surveys/inspection/investigation reports and laboratory analytical results.
- Payroll information, financial and budgetary information.
- Operating Plans, Business Plans and Accountability Reports below the corporate level.
- Security investigations performed by Corporate Security Services or AISOD's Technical Services group, unless classified at a higher level.
- Active and historical audit data, unless classified at a higher level.
- Seismic Sections - Geological cross-sections and other information (Maps/Documents) showing seismic data or wells with geological information.
- Aerial photographs, maps or other like information that does NOT disclose the location and configuration of military or other vital government installations or equipment or the location, or configuration of Company producing, manufacturing or transportation facilities but is required for Company business related activities.

* **Storage/Destruction Guidelines:**

Departments shall establish procedures for the handling, retention and storage of "Restricted" information to protect it from unauthorized disclosure, distribution or misuse. Minimum requirements for these procedures are as follows:

- Hardcopy "Restricted" information should be secured against access by unauthorized persons when not in use and stored in a secured environment or kept in a lockable desk/cabinet.
- Electronic information stored in files on personal computers (PCs) should be password protected.
- Access to electronic information should be controlled using IT recommended access control software and procedures.

- Users should lock PCs when away for extended periods of time.
- Electronically stored "Restricted" information should be routinely backed up or deleted using IT recommended procedures.
- Hardcopy "Restricted" information, when not required should be destroyed through a shredder so that it is no longer usable or recognizable after its retention period has elapsed.
- Electronic storage devices containing "Restricted" information should be sanitized in accordance with GI 2.99.210 (Sanitization and Disposal of Saudi Aramco Electronic Storage Devices and Obsolete/Unneeded Software).

* For detailed standards and recommendations on "Restricted" information storage/physical destruction, consult ISP&SSD (hardcopy information). Destruction of "Restricted" information in bulk quantity shall be witnessed and certified by AISOD personnel upon written request supported by form SA-9546 from the proponent or user organization. CSS can be consulted for destruction of computer devices and other electronic items that contained sensitive information.

7.4 **Confidential information:**

Criteria:

- Disclosure of this information could have a serious financial impact on the Company.
- Disclosure could impact the competitive position of the Company.
- Disclosure could seriously impair the operational effectiveness/strategies of the Company.
- Disclosure could embarrass the Company and adversely affect its image and reputation.

* **Examples:**

- Information showing oil and gas reserves.
- Complete Exploration Prospect Packages, forecast production, refining and export delivery levels and capabilities.
- Corporate level Operating and Business Plans.
- Reports to the Board of Directors and Management Committee.
- Security investigations involving fraud, major thefts, and conflicts of interest.
- Plans for major expansion and development projects and programs.
- Business and trade secrets.
- Ground or aerial photographs, maps or other like information that discloses the location and configuration of Company producing, manufacturing and transportation facilities.
- Proprietary and other information that if released may violate contractual or legal restrictions on disclosure, including information covered by a formal Confidentiality Agreement or similar undertaking towards a third party.
- Confidential contracting and purchasing information, including contractor/vendor bids and bid tabulations, contract and purchase order awards and award recommendations, contract dispute proceedings and settlement recommendations, etc.
- Confidential customer information.
- Personnel files.
- Supplemental contractors manpower and other service contracts.
- Information whose disclosure could compromise the security of the Company's facilities or its personnel, including vital installation drawings that are not classified at a higher level.

- Medical confidential information containing patient-related medical information will be classified as such and will follow the policies and procedures outlined in medical services policies as established by the Saudi Aramco Medical Services Organization.
- Proprietary information relating to Saudi Aramco Intellectual Property.

* **Storage/Destruction Guidelines:**

Departments shall establish procedures for the handling and storage of "Confidential" information to protect it from unauthorized disclosure, distribution or misuse. Minimum requirements for these procedures are as follows:

- The same guidelines and requirements for the storage/destruction of "Restricted" information shall apply to "Confidential" information. See 7.3 for details.
- Destruction of "Confidential" information in bulk quantity shall be witnessed and certified by AISOD personnel upon the written request supported by form SA-9546 from the proponent.

* For detailed standards and recommendations on "Confidential" information storage/destruction, consult ISP&SSD for hardcopy information. Consult CSS for destruction of computer devices and other electronic items that contained sensitive information. Refer to GI 299.120 (Sanitization and Disposal of Saudi Aramco Electronic Storage Devices and Obsolete/Unneeded Software) for more details.

7.5 **Government Confidential information:**

Criteria:

- Disclosure may impact the security of not only the Company but also the Kingdom; or may negatively impact the Kingdom's political interests, foreign relations, income and/or the business environment generally.

Examples:

- Ground or aerial photographs, maps or other like information disclosing the location and configuration of military or other vital government installations or equipment.
- Highly sensitive government correspondence from senior officials.
- Information related to or descriptions of Company installations which are critical to the overall continuity of oil/gas production or distribution.
- Information which, if released, could affect the political interests, foreign relations, income or reputation of the Kingdom.

* **Storage/Destruction Guidelines:**

Departments shall establish procedures for the handling and storage of "Government Confidential" information to protect it from unauthorized disclosure, distribution or misuse. Minimum requirements for these procedures are as follows:

- Procedures and requirements for the destruction and storage of information classified as "Government Confidential" are the same as those listed in 7.3 and 7.4 above. Furthermore, Saudi Aramco Affairs or Industrial Security, as appropriate, should be consulted before any "Government Confidential" information is destroyed.
- Destruction of "Government Confidential Information" in bulk quantity shall be witnessed and certified by AISOD personnel upon the written request supported by form SA-9546 from the proponent.
- For detailed standards and recommendations on "Government Confidential" information storage/physical destruction, consult ISP&SSD (hardcopy information). Consult CSS for destruction of computer devices and other electronic items that contained sensitive information. Refer to GI 299.120 (Sanitization and Disposal of Saudi Aramco Electronic Storage Devices and Obsolete/Unneeded Software).

8.0 LABELING PROCEDURES FOR SENSITIVE INFORMATION AND DOCUMENTS

8.1 An appropriate set of procedures must be developed and implemented by each responsible proponent organization, for information labeling and handling in accordance with its classification. These procedures should cover

information in physical and electronic formats. For each classification category these procedures should include guidelines for the following activities:

* 8.1.1 Copying (hardcopy or electronic)

* 8.1.2 Storage (hardcopy or electronic)

8.1.3 Transmission by post, fax, e-mail and the Internet

8.1.4 Backup and disaster recovery

8.1.5 Destruction

8.2 All hardcopy information that is classified as "Confidential" or "Government Confidential" must be conspicuously labeled as such. Information and documents classified as "Restricted" may or may not be labeled at the discretion of the proponent organization.

***** 8.3 Hardcopy sensitive Company information that must be labeled shall be identified with the highest level of classification (see section 4.3 through 4.5) at the top center of every page and volume in the document (for hard copies, plans, summaries, project reports, survey reports and photographs, etc.). All pages of each labeled sensitive document must be numbered according to a reasonable scheme, i.e., 'x of y' (page 1 of 25) or sequential order (1, 2, 3 …) so that missing pages can readily be discovered. Photographs of a sensitive nature should be labeled and numbered on the reverse side. Drawings should be labeled according to Saudi Aramco Engineering Procedures (120 and 127). Aerial photographs will be labeled in the most cost-effective method, as defined by the proponent.

***** 8.4 Some information in electronic form, data residing in a database, information displayed on intranet or Web page, etc., cannot be physically labeled and electronic means of labeling must be used instead. Examples are:

8.4.1 The use of a label in a footer or header of a document.

8.4.2 A watermark displaying "Confidential" in background of an intranet or Web page.

8.4.3 A notice or warning statement that displays before accessing data in a database.

***** 8.5 Mark e-mail as "Confidential" using the built-in function of the e-mail client and displaying the label at the top of the message. Refer to GI 299.200 for providing standards on e-mail disclaimer statement.

8.6 Sensitive information in electronic formats is considered to have an implied label when protected by a secure access control method. Sensitive information that is required to be labeled shall be identified with its highest level of classification (see section 4.3 through 4.5).

9.0 RELATED DOCUMENTS FOR REFERENCE

Related Company documents concerning the protection of Company information include:

***** 9.1 INT-7 (Data Protection and Retention), INT-9 (Intellectual Property) and corporate policy statement on Corporate Systems Security.

***** 9.2 Information Protection Manual provides the material necessary to implement the Corporate Policy Statement on Computer Systems Security.

9.3 Saudi Aramco Records Management Manual includes Information Management Guidelines and describes record retention, information life, storage, retrieval and destruction and the general responsibilities of the organizations involved in information management.

9.4 Conflict of Interest and Business Ethics Policies (SA-8942) describe employees' responsibilities for the protection of confidential and internal Company information according to ethical and legal standards.

9.5 Industrial Relations Manual describes the release of employee personal information, gives examples of conflict of interest and explains disclosure procedures.

9.6 Internal Controls and the Role of Internal Auditing in Saudi Aramco "Summary of Essential Internal Controls".

****** 9.7 Saudi Aramco Computer Use Policy for Employees (SA-9595) and Non-Employees (SA-9696).

9.8 Saudi Aramco Engineering Procedure (SAEP) 120 provides guidelines and procedures for preparing security drawings of Saudi Aramco vital facilities. SAEP-127 details the procedure for controlling original engineering and

vendor drawings when Saudi Aramco personnel utilize them and covers the security and control of original engineering and vendor drawings and the confidentiality of sensitive documents when they are in the custody of organizations outside of Saudi Aramco.

** 9.9 Intellectual Assets Management guidelines which detail the instructions for record-keeping of information for intellectual property and patent protection.

* 9.10 Medical Services Policies: MSP-231, "Confidentiality of Patient Information" and MSP-232, "Release of Medical Records, Medical Reports and Disclosure of Patient Information."

10.0 CONTACT INFORMATION OF CONCERNED PARTIES

Special Security Services Division - Industrial Security Planning & Support Services Department
Box 90, Dhahran
Tel: 03-876-2815, Fax: 03-876-6660

Information Protection Division
Building 3134, Room 3 – LIP, Dhahran
Tel: 03-872-9258, Fax: 03-872-9212

Corporate Security Services
Room T-800, Tower Building, Dhahran
Tel: 03-874-5955, Fax: 03-873-3909

** Intellectual Assets Management Group
Building 2298, Room 115A, Dhahran
Tel: 03-872-5215/03-872-5213, Fax: 03-872-6140

Approved:

Date: _____

_____
PRESIDENT & CHIEF EXECUTIVE OFFICER