CONTENT:

This General Instruction (GI) outlines the Saudi Aramco Electronic Mail (Email) Use and defines the needed controls to ensure that the Saudi Aramco email service is used in an appropriate and legitimate manner. The text of this Instruction contains:

1. PURPOSE

This General Instruction sets forth the appropriate and legitimate use of any email sent from a Saudi Aramco email address or email sent utilizing the Saudi Aramco electronic mail (email) infrastructure.

* All comments and questions relating to this General Instruction should be directed to Information Protection Management Division (IPMD).

2. SCOPE

This General Instruction applies to all users, holders, and uses of Saudi Aramco electronic mail systems and all electronic mail systems and services provided or owned by Saudi Aramco.

3. DEFINITIONS

* IPMD: Information Protection Management Division
* IPCD: Information Protection Center Division
CSSD: Corporate Security Services Division
CSA: Computer Security Administration
CSL: Computer Security Liaison
Saudi Aramco Email Systems or Services: Electronic mail systems or services owned or operated by Saudi Aramco

** Cyber Law: IT Crime Control and the Electronic Transaction regulations

4. ACCEPTABLE USE

* Saudi Aramco's email systems must be used in a responsible, ethical and legitimate manner. Occasional and incidental personal email use is permitted if it does not interfere with the work of personnel, the Company's ability to perform its mission, directly or indirectly interfere with Saudi Aramco operation of computing facilities or electronic mail services, does not consume more than a trivial amount of resources and is in compliance with this G.I.

5. EMAIL SPAM

The sending of identical or nearly identical messages to a large number of recipients such as to thousands (or millions) of recipients (email spam) is strictly prohibited. This includes the unsolicited sending of commercial or bulk email to individuals who did not specifically request such material. Spam mail can be reported to anti-spam@aramco.com.

6. VIRUS CHECKING

Any files or attachments received from non-company sources must be scanned with the company's virus detection software before opening. The current corporate anti-virus solution, to scan email messages, is embedded within the corporate email client. Users should not open emails or attachments from unknown senders and delete these immediately.

7. EMAIL FORWARDING

The automatic forwarding of electronic mail to email services outside Saudi Aramco is prohibited. Users of Saudi Aramco's email system must make use of the Saudi Aramco Extranet email facility to access email within its system when operating outside Saudi Aramco, e.g. traveling abroad. The use of external email services for Saudi Aramco business is also prohibited unless authorized.

8. EXTERNAL REPRESENTATION

* Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Saudi Aramco unless appropriately authorized (explicitly or implicitly) to do so. The sending of inappropriate messages could be harmful or tarnish the reputation of Saudi Aramco. When participating in newsgroups, mailing lists, social networks and email discussions, employees may disclose their affiliation with Saudi Aramco but in doing so they agree to be bound by Company guidelines that protect the image of Saudi Aramco.

9. ARCHIVING AND RETENTION OF EMAIL

The corporate policy INT-7 requires that; Data, however recorded, will be retained as long as required for operational, legal or disaster recovery purposes. Departments should devise their own email retention policy for their own operational and legal requirements in line with INT-7. Email retention can be achieved by copying all business emails to a file server or designated email account.

* In general users should keep a repository of business emails, e.g. .pst file, on their computers or on the corporate File and Print servers where back-up can be performed. Upon leaving the company a copy should be provided to the CSL. The time for retention should be decided based on the operational or legal requirements of the particular department.

Email, on Saudi Aramco email servers, will be retained for 30 days after a user has left the company.

10. EMAIL SUSPENSION

* An email account may be suspended, or access to Saudi Aramco electronic mail services restricted/blocked, without prior notice and without the consent of the email user, when there is substantiated reason to believe that violations of this G.I. or law have taken place, risk of liability to Saudi Aramco exists, or when failure to act could seriously impede Saudi Aramco's business operations. IPMD can authorize an immediate temporary suspension of a user's email account. CSSD can authorize a suspension with an official security case number. Also, User's department manager or higher can authorize the suspension of only the sending functionality of his user's email account when deemed necessary.
Access for a user to his/her email will be suspended if the user leaves the company or his/her contract expires with Saudi Aramco.

11. EMAIL DISCLAIMER

All email to the outside world, non Saudi Aramco email addresses, should have the following approved disclaimer:

"*The contents of this email, including all related responses, files and attachments transmitted with it (collectively referred to as "this Email"), are intended solely for the use of the individual/entity to whom/which they are addressed, and may contain confidential and/or legally privileged information. This Email may not be disclosed or forwarded to anyone else without authorization from the originator of this Email. If you have received this Email in error, please notify the sender immediately and delete all copies from your system.*

Please note that the views or opinions presented in this Email are those of the author and may not necessarily represent those of Saudi Aramco. The recipient should check this Email and any attachments for the presence of any viruses. Saudi Aramco accepts no liability for any damage caused by any virus/error transmitted by this Email."

* This disclaimer may be changed, or a different disclaimer approved, at the discretion of IPMD with concurrence from LAW Department.

12. EMAIL ADDRESS FORMAT

* The current format of Saudi Aramco corporate email addresses is name.lastname@aramco.com, with the possibility that a number may be added to ensure uniqueness. The format can be changed if deemed necessary for operational or legal purposes pending review and approval by IPMD.

13. COPYRIGHT

All Saudi Aramco employees, contractors, or other users are required to respect the copyrighted materials of others and only use such copyrighted materials with necessary permission.

14. BUSINESS ACCESS TO EMAIL

* Business access to a user's email, or disclosure of a user's email, without the consent of the user, will only be permitted in one of the following instances:

1. It is required in support of an official security investigation by CSA/CSSD.
2. User is absent and his department has a business justification of accessing the user's email. (Requires a written request signed by the user's department head or higher management level.)

* In the case where a user is absent and his department has a business justification, as described in 2, the following process needs to be followed. A letter with manager approval needs to be forwarded to AMD requesting the access with the business justification. During the recovery of the email, a management-designated representative from the requesting department, who should be the CSL, must be physically present. Only the needed email will be recovered and the representatives will not access any email that is not related to the business justification. The user will be notified of this action at the earliest possible opportunity by the CSL or other management-designated representative.

15. NO PRESUMPTION OF PRIVACY

* All communications transmitted or received through the Company's email systems using Company facilities are considered the property of Saudi Aramco. The Company reserves the right to access, monitor and examine any messages transmitted or received over the Company's communication networks. Email communications should not be assumed as private and as such privacy should not be expected.

16. CLASSIFIED AND PROPRIETARY INFORMATION

* Users must not transmit classified or proprietary Company information (see Intellectual Assets Management website http://iam.aramco.com.sa) to unauthorized sources. Users must take the necessary precautions to protect classified information from disclosure in accordance with GI-710.002 and GI-0850.006. Information classified as **Restricted**, **Confidential** and **Government Confidential** as defined in GI-710.002 must be encrypted before transmission by email. See Encryption Security Standards & Guidelines on IPMD website.

17. EXAMPLES OF PROHIBITED ACTIVITIES

17.1. Sending of unsolicited commercial email, unsolicited bulk email, unsolicited email or forwarding of chain letters.

17.2. The creation or distribution of any illegal, unethical, offensive or disruptive messages, including messages containing pornography, abusive language or offensive comments about national origin, political or religious beliefs.

17.3. Distribution of destructive or fraudulent code or intentional insertion of viruses.

17.4. Any form of pornography or other items deemed illegal by the Company or the Government of Saudi Arabia.

17.5. Activities supporting a commercial business which are not authorized by the Company or Government authorities.

17.6. Unauthorized distribution of copyrighted material including, but not limited to, copyrighted music, photographs, books or other copyrighted materials.

17.7. Unauthorized use, or forging, of email header information.

* 17.8. Sending messages to large numbers of recipients without proper authority. Proper authority may include direct management, Services Management Division, etc. The sending of messages to large numbers of recipients, if the messages do not concern the majority, is also prohibited.

17.9. Sending messages containing political support or political content.

17.10. Directly or indirectly interfering with Saudi Aramco's operation of computing facilities or email services.

17.11. Bringing the Company into disrepute, or exposing it to negative publicity or any other harmful effects.

17.12. “Spoofing”, i.e., constructing an electronic mail communication so it appears to be from someone else.

** 17.13. “Phishing”, e.g., an email disguised as an official e-mail from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website.

** 17.14. Use of Saudi Aramco email groups (distribution lists) to send non-business related emails or bulk emails to users.

** 17.15. Using a third part email service to send unsolicited or bulk emails (SPAM) to Saudi Aramco users.

** 17.16. Using the email in violation of the Saudi Arabia Cyber Law.

18. VIOLATIONS

Any employee found to have violated this GI may be subject to disciplinary action, up to and including termination of employment, referral to law enforcement agencies or other appropriate administrative or legal action.

Date: _____ Recommended By: _____
Administrator,
Information Protection Management Division

Date: _____ Recommended By: _____
Manager,
Information Protection & Technology Planning Dept.

Date:_____ Approved By: _____
Executive Director,
Information Technology