CONTENT:

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

01. Purpose
02. Scope
03. Definitions
04. Acceptable Use
05. Requesting Internet Access
06. Suspending Internet Access
07. User ID and Password Control
08. Logging and Access to Internet Logs
09. Internet Services
10. No Presumption of Privacy
11. Publishing
12. External Representation
13. Copyrights
14. Virus Checking
15. Junk Email
16. Reporting Security Problems
17. Examples of Prohibited Activities
18. Violations

1. PURPOSE

This General Instruction sets forth the use of Internet by users through the Saudi Aramco Internet connection. It defines acceptable and prohibited use of the Internet.

* 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 accessing the Internet through the Saudi Aramco provided internet connection only (Business Internet as defined in section 3 below). The fact that prohibited activities can be performed without use of the Saudi Aramco Internet connection does not excuse employees from complying with all applicable Company procedures and regulations.

This document excludes Home Internet use as defined in section 3 below.

3. DEFINITIONS

Home Internet: is an isolated segment of the Saudi Aramco Internet connection designed to provide Internet services to its employees and their dependants. All Saudi Aramco regular employees are eligible to receive this privilege.

Business Internet: is the production network segment designed to provide Internet services to connected business users. This GI applies to all business Internet access, regardless of the method of access (dial-up, call-back, wireless, ADSL, etc.) or the place from which it is accessed (the office, employee's residence, library, dining halls, etc.)

* IPMD: Information Protection Management Division
* IPCD: Information Protection Center Division
** AMD: Access Management Division-
CSA: Computer Security Administration
CSSD: Corporate Security Services Division
** CITC: Communications & Information Technology Commission
** Cyber Law: IT Crime Control and the Electronic Transaction regulations

4. ACCEPTABLE USE

Saudi Aramco advocates the use of Internet by all authorized users for business and self-development. Saudi Aramco provides Internet access to facilitate the conduct of corporate business. Occasional and incidental personal Internet use is permitted if it does not interfere with the work of personnel, the corporation's ability to perform its mission, does not consume more than a trivial amount of resources, does not interfere with the user's productivity and is not amongst activities listed in Section 17 of this GI.

5. REQUESTING INTERNET ACCESS

* All users accessing the Internet through the Saudi Aramco Internet connection **must** sign the Saudi Aramco Computer Use Policy (SA-9595 or SA-9696 for Non-Employees) and must follow company procedure to obtain access to the Internet.

6. SUSPENDING INTERNET ACCESS

* Department Heads may request the suspension of Internet access, in writing from AMD, for specific employees. IT Helpdesk, IPMD or Corporate Security Services Division can also request the suspension of Internet access in the case of abuse or threat. This must be reported to the employee as soon as possible.

7. USER ID AND PASSWORD CONTROL

A user ID is employed to uniquely identify every Internet user. Users shall not share or disclose their password or authentication codes to anyone. The user must take reasonable steps to safeguard his/her authentication codes. Users shall take precautions to ensure that no other person makes use of an Internet session established with their user ID and password.

8. LOGGING AND ACCESS TO INTERNET LOGS

All web sites accessed by a user shall be logged by IPCD and the logs kept for a minimum of twelve (12) months. IPCD shall examine these logs regularly and compile a list of top abusers accessing objectionable material. The list shall be forwarded monthly to Corporate Security Services Division for their action. The release of the Internet access logs is controlled by the Log Administrator (IPCD) only. Corporate Security Services Division or IPMD may request these logs in writing only if a case number has been assigned. The request will have to clearly define the purpose for requiring the logs. No other entity or individual is allowed access to the Internet logs or is authorized to request Internet logs.

9. INTERNET SERVICES

The Internet offers a host of services (ports) e.g. telnet, ftp, newsgroups, etc. Several of these services are blocked to protect the Saudi Aramco network. The opening of any Internet services (ports) can be requested, in writing or email, from IPCD. The opening of any Internet service (ports) must be approved by IPCD.

10. NO PRESUMPTION OF PRIVACY

All communications transmitted or received through the Saudi Aramco Internet connection are considered the property of Saudi Aramco. The Company reserves the right to access, monitor and examine, by its authorized personnel, any communications transmitted or received over the Saudi Aramco Internet connection.

11. PUBLISHING

Users must not upload, publish, transmit or otherwise disclose any company material on or through the Saudi Aramco Internet connection unless authorized. Company material intended for publishing or posting on the Internet shall be subject to review by Public Relations Department prior to publishing or posting. Company information is also governed by existing policies (Records Management Manual 1996; GI-850.006; INT-7; GI 710.002). Unauthorized publication of company material classified as Company General Use, Restricted, Confidential or Government Confidential as defined in GI-710.002 on the Internet is prohibited.

12. EXTERNAL REPRESENTATION

* Employees should take the necessary care when participating in newsgroups, mailing lists, social networking websites, chat sessions and other offerings on the Internet not to disclose their affiliation with Saudi Aramco. Whenever employees provide an affiliation, unless they have been expressly designated as a spokesperson of Saudi Aramco, they must clearly indicate the opinions expressed are their own, and not necessarily those of the Company.

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. VIRUS CHECKING

* Any files downloaded from non-Saudi Aramco sources via the Internet must be scanned with the Company's virus detection software before opening. Any viruses found, and not removed by virus software, should be immediately reported to the IT Helpdesk.

15. JUNK EMAIL

Users are prohibited from using the Saudi Aramco Internet connection for the transmission of unsolicited bulk email advertisements or commercial messages. When users receive unwanted and unsolicited email (also known as spam), they must refrain from responding directly to the sender. Refer to the GI 299.200 (Saudi Aramco Email Use) for further details.

16. REPORTING SECURITY PROBLEMS

* If any unauthorized use of Saudi Aramco's Internet connection has taken place, or whenever any intrusion attempt, hacking, or port scans are being detected, or whenever passwords or other system access control mechanisms are lost, stolen, or disclosed it can be reported as outlined in Information Security Incident Management Standards and Guidelines available on IPMD Website.

17. EXAMPLES OF PROHIBITED ACTIVITIES

Prohibited activities when accessing the Internet through the Saudi Aramco internet connection include, but are not limited to, the following:

* 17.1 Browsing Internet sites that contain pornographic, adult material, gambling, prohibited drugs, violence, illegal substances, extremist/militancy, racism, indecent, abusive, defamatory, or hate-based web sites, and hacker or malicious and harmful web sites.

** 17.2 Accessing Internet sites or resources in contravention of the CITC regulations with regards to Internet use within Saudi Arabia.

** 17.3 Using the Internet in violation of the Saudi Arabia Cyber Law.

17.4 Posting, sending, or acquiring pornographic, extremist/militancy, abusive, hate-based or hacker-related material.

17.5 Conducting or promoting a personal business for commercial purposes.

17.6 Engaging in unlawful or other activities, which would bring discredit to Saudi Aramco.

17.7 Unauthorized access or attempts to break into any computer (masquerade, cracking, hacking, etc.), whether of Saudi Aramco or another entity.

17.8 Using tools or utilities to intercept, interrupt, "sniff" or monitor the network without the proper company authorization. Authorizations for such activities must be documented and approved by IPMD.

17.9 Using the Saudi Aramco Internet connection to perform any act that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, Saudi Aramco or any person.

* 17.10 Interference with or disruption of Company computer or communications systems such as consuming the company internet bandwidth by massive download of non-business materials.

17.11 Accessing the corporate network via any unauthorized modem or other remote access service.

17.12 Publishing personal information concerning company employees.

17.13 Establishing unauthorized connections to the corporate network that could allow users to gain access to Saudi Aramco's systems and information.

18. VIOLATIONS

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

APPROVAL

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

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

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