CONTENT

This General Instruction establishes the different connections that may be used to access Saudi Aramco computer systems or corporate network from a remote location. It also sets the requirements that must be in place before a remote connection is authorized and sets the minimum standards that must be implemented for remote connectivity.

1. PURPOSE

Remote access to Saudi Aramco's corporate network and computing resources must be managed carefully to ensure that only authorized users can connect to the Saudi Aramco network and that these connections are protected and secure. This General Instruction limits these connections to company approved remote access connections and establishes the minimum security requirements for these connections.

2. SCOPE

This document applies to:

1. All Remote Access connections to the Saudi Aramco corporate computer systems and networks
2. All entities utilizing Remote Access.

3.

DEFINITIONS

Affiliates and Subsidiaries: Affiliates and Subsidiaries of Saudi Aramco as defined in the Saudi Aramco Management Guide.

Contractors: Persons who are contracted by Saudi Aramco as individuals or by a company contract.

Remote access: Access to the Saudi Aramco's computer systems or networks from a location outside the company's control by authorized individuals or entities.

Saudi Aramco Users: Users in possession of a valid Saudi Aramco ID (badge) number e.g. Saudi Aramco employees and contractors

Third Parties: Users not in possession of a valid Saudi Aramco ID (badge) number e.g. vendors, customers, Joint Venture companies, etc. who have a requirement to access the Saudi Aramco network for business or maintenance purposes.

Citrix: A service that provides remote access by either publishing applications or VPN

4. ABBREVIATIONS

AITD: Area Information Technology Department
DNED: Data Network Engineering Division
IPCD: Information Protection Center Division
IPMD: Information Protection Management Division
WID: Windows Infrastructure Division
MPLS: Multi Protocol Label Switching
IP-VPN: Internet Protocol – Virtual Private Network

5. REMOTE ACCESS TO SAUDI ARAMCO COMPUTER SYSTEMS OR NETWORKS

Remote Access to and from Company-owned computer systems and networks may be authorized to support operational and business requirements where there are no legal restrictions, where other alternatives are not practical or cost effective, and when adequate means to protect corporate data can be designed. No direct or indirect remote access is permitted to those high-performance computers which have an existing international export license agreement with the US Department of Commerce, Bureau of Industry and Security. Remote access to these computers must comply with the provisions of their individually controlling Security Safeguard Plans (SSPs).

6. COMPANY APPROVED REMOTE ACCESS CONNECTIONS

Only company approved remote connections are allowed to provide remote connectivity to the corporate network and users **must** only use company-approved remote connections for remote access. Requests for other Remote

Access connections must be approved by Information Protection Management Division. The current company approved Remote Access Connections are listed in Table 1.

TYPES OF SAUDI ARAMCO REMOTE ACCESS CONNECTIONS		
Company Approved Remote Access Connections	**Reference**	**Standards & Guidelines**
Extranet	See 6.1	Extranet Security standards and Guidelines
Wireless **(VSAT, GSM, 802.11, etc)**	See 6.2	Wireless Network & Portable Device Security Standards and Guidelines
VPN **End User to Saudi Aramco VPN** **Site-Site VPN**	See 6.3	VPN Security Standards and Guidelines
Published Application Remote Access (Citrix)	See 6.4	Defined in this GI
Business Dialup Modem Access	See 6.5	Defined in this GI
Leased Circuits **Point-Point Links** **IP- VPN (MPLS)Links**	See 6.6	Defined in this GI
Other	See 6.7	Other remote connections may be approved by IPMD pending a risk management analysis and business justification.

Table 1: Current Company Approved Remote Access Connections

6.1. Extranet: The Saudi Aramco Extranet has been designed to give remote users limited access to specific applications or information. The Extranet is a protected environment with the necessary security controls. For more information see Extranet Security Standards and Guidelines available on IPMD website. Users in possession of a Saudi Aramco ID (badge) number and valid network ID are granted automatic access to the Saudi Aramco Extranet (http://www.aramco.com) for authorized services. Third parties' access must be sponsored by a department within Saudi Aramco and will need sponsoring manager approval to utilize this service. Web pages that have been classified as public, reside on the Extranet and approved by Public Relations Department (PRD) can be accessed from the Internet without any authentication.

6.2. Wireless: Wireless networks can be a cost effective alternative to cabled networks and provide personnel with mobile connectivity. Wireless networks can be utilized in Saudi Aramco if approved and configured in accordance with company guidelines. For more information see Wireless Network and Portable Device Security Standards & Guidelines available on IPMD website. This service is restricted for **authorized** users only. Third parties must be sponsored and approved by a department within Saudi Aramco.

6.3. VPN: VPN Connections are classified as either End User to Saudi Aramco or Site-to-Site for the purpose of this General Instruction. They are described below:

6.3.1. End User to Saudi Aramco VPN:
This is a Virtual Private Network that securely connects users and ensures that only authorized users can access the network and that the data cannot be intercepted. This service is restricted for Saudi Aramco users with department manager approval. Third parties will need to complete the Third Party VPN Service Request form (SA-9649) with sponsoring department manager approval to utilize this service. IPCD must review and approve this service. WID will archive and document all third parties utilizing this service.

6.3.2. Site-to-Site VPN:
This is a Virtual Private Network that allows a company to securely connect to Saudi Aramco's network for dedicated access. Site-to-site VPN connections must terminate at the corporate perimeter VPN gateway. Applicants need to complete and sign the Third Party VPN Service Request form (SA-9649). These connections must be reviewed and approved by IPCD and required engineering design packages are created by DNED. All active site-to-site VPN connections must be archived by DNED.

6.4. Published Application Remote Access: Citrix allows authorized users to access specific applications or services as approved. It allows authorized users to remotely access corporate applications, desktops and services. This service is restricted for **authorized** users only. Third parties must be sponsored by a department within Saudi Aramco and will need sponsoring manager approval to utilize this service.

6.5. Business Dialup Modem Access

In exceptional cases where no other alternatives exist, a direct modem to modem connection between an external entity and a modem located in Saudi Aramco can be approved and authorized by IPCD.

6.5.1 Approval and Registration: No modem to modem connection to the corporate Saudi Aramco network, computer systems and workstations are allowed without prior approval of IPCD. Applicants requesting a direct modem to modem connection must complete the Computer Dial-up Service Request form (SA-9204), available from IPCD, with department manager approval and forward it to IPCD for approval.

6.5.2 Monitoring: IPCD will scan the list of telephone numbers within Saudi Aramco occasionally to detect any unauthorized modems. If a modem is found not listed in the registered list of approved modems they will contact the relevant department for clarification and remediation. Telephone lines with unauthorized modems will be disconnected by AITD appropriate division after user notification and no appropriate action taken.

6.6. Leased Circuits:
A leased circuit includes Point-Point links or Internet Protocol VPN (MPLS) links and may be approved to connect National and International Aramco offices, Aramco international affiliates and approved third party offices to the Saudi Aramco network. The remote network, connected to the Saudi Aramco network, must be isolated from other third party networks with adequate physical security/access control to the building or office hosting the remote network. Computers connected to the remote network must use the Saudi Aramco image and be under the control of IT. Applicants for a national and international leased circuit must contact DNED for approval.

6.7. Other: In exceptional circumstances, other remote access connections may be requested from DNED. DNED will issue an engineering package if required and forward it to IPMD for approval pending a risk management analysis.

7. GENERAL GUIDELINES

7.1. A signed contract **must** exist between Saudi Aramco and any third party entity utilizing or requiring remote access. An electronic "Terms of Use" can also be utilized. The signed contract or electronic "Terms of Use" must include a non disclosure agreement and an appropriate use agreement similar to SA-9696.

7.2. Remote Access User IDs must be maintained in accordance with Computer Accounts Security Standards & Guidelines available on IPMD website.

7.3. The sponsoring department, e.g. sponsoring department CSL, must notify IT Helpdesk when access is no longer required for any specific user. IT Helpdesk will coordinate with the applicable Access Control group to communicate the deletion of User IDs when notified.

7.4. Users should take the following precautions when accessing Saudi Aramco systems remotely from public areas:

a. Do not leave the computer/session unattended.
b. Pay attention to who is watching over your shoulder.
c. Choose reputable public computer places.
d. Delete temporary files/cookies and terminate browser session.
e. Do not save any Saudi Aramco sensitive information on the local drives of the public computer.
f. Permanently delete any downloaded Saudi Aramco documents/data at the end of your session.

8. PUBLISHING

Proponents of applications that provides remote access **must** review and adhere to GI-710.002 and GI-850.006 (see http://gi.aramco.com.sa), pertaining to the Classification of Sensitive Information, before publishing any information on remote access applications or allowing any access to company resources.

9. AUTHENTICATION

Authentication for remote access **must** be strong. All users utilizing remote access **must** be identified and authenticated. Authentication should be done using the corporate trusted database of user id's and passwords e.g. Active Directory. Authentication should include the use of digital certificates or any other approved authentication methods. Remote Access Connections should have the functionality to enable remote users to change their passwords.

10. USER AGREEMENT

All users requesting access to the Saudi Aramco network via remote access **must** sign the Saudi Aramco Computer Use Policy (SA-9595) or other IPMD approved Computer Use agreement, unless a signed contract is in place with

sufficient terms. Saudi Aramco Subsidiaries must use their own proprietary Computer Use Policy form that is approved by IPMD. Subsidiary and affiliate companies refer to section 15.

11. AUDIT LOGS

All Remote Access **must** be logged and as a minimum the logs will include the user ID, date and time of access, duration of access and originating IP address. . (See Audit Log Security Standards & Guidelines on IPMD website)

12. INFORMATION OBTAINED THROUGH REMOTE ACCESS

Remotely-accessed information must be protected from unauthorized access or disclosure. Proper protective measures include securing materials when unattended and shielding materials from unauthorized viewing. Proper disposal measures include the shredding or destruction of sensitive information prior to disposal.

13. ENCRYPTION

Information must be encrypted in accordance to GI-710.002 when transmitted between the remote location and target host.

14. RESTRICTION OF ACCESS

All Remote Access **must** be restricted to the minimum services and functions required where feasible. Access **should** be limited to the specific network segment(s) and applications for which their access is justified. The principle of least required access privileges must be followed.

15. TIMEOUT

End user remote access sessions **must** enforce session time-out. This time-out **must** terminate all sessions that have had no activity for a maximum period of 20 minutes.

16. REMOTE ACCESS FOR SAUDI ARAMCO AFFILIATES OR SUBSIDIARIES

Saudi Aramco affiliates and subsidiaries may be granted logical access to the Saudi Aramco corporate network if they are in possession of a valid badge number registered with Saudi Aramco Industrial Security Organization and the conditions below are met. Affiliates or subsidiaries requiring logical access, except for ASC and AOC, must contact Industrial Security Organization to sign a mutual agreement.

- Affiliate employees will only be granted remote access to Saudi Aramco's systems if they have signed the Saudi Aramco Computer Use Policy Form SA-9696 or other IPMD approved Computer Use Policy. Subsidiary employees must sign their own proprietary Computer Use Policy form. The initial Computer Use Policy form must be filed and accepted by IPMD.

- Affiliate or subsidiary employees that are granted logical access to Saudi Aramco systems must adhere to Saudi Aramco's General Instructions, Standards & Guidelines and Procedures regarding IT systems. These documents can be found at IPMD website.

- In the case of abuse of Saudi Aramco systems or violations of the General Instructions and Standards & Guidelines, the matter will be reported to the Affiliate or subsidiary management. It is expected that Affiliate or subsidiary will give the necessary cooperation to assist in such an investigation and that appropriate steps will be taken by the Affiliate or subsidiary to remedy the situation.

- In the case where Saudi Aramco computer systems are located at Affiliate or subsidiary premises the Affiliate or subsidiary management is responsible to ensure that appropriate physical controls/procedures are in place to prevent unauthorized physical access to the systems.

17. MONITORING

The monitoring of remote connections should be done in accordance with Computing Monitoring and Reporting Security Standards and Guidelines available on IPMD website. In addition Remote Access Connections should employ Intrusion Detection/Prevention Systems, where applicable, to monitor these connections.

18. VIOLATION

Any user or entity 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: _____ Concurred By: _____

Manager,
Information Protection & Technology Planning Department

Date _____ Approved By: _____

Executive Director,
Information Technology