

Standard for Third Party Network Connectivity

NOVEMBER 2007



Standard for Third Party Network Connectivity

Corporate Affairs Department

NOVEMBER 2007

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

Users of this recommended practice should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgement should be used in employing the information contained herein.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, N.W., Washington, D.C. 20005.

Copyright © 2007 American Petroleum Institute

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Suggested revisions are invited and should be submitted to the Director of Corporate Affairs, API, 1220 L Street, NW, Washington, DC 20005.

Table of Contents

Standard	3
Trust	4
1 Connection Request & Agreement Checklists.....	6
1.1 API Third Party External Network Connection Request Checklist.....	6
1.2 Third Party Connection Terms and Conditions Checklist.....	7
1.3 API External Network Connection Detailed Request Checklist	8
1.4 API Third Party User Responsibility Sample Agreement.....	9
1.5 External Network Connection Information Sample Request Form	13
2 Risk Analysis Template.....	16
2.1 Executive Summary	16
2.2 General Connection Information.....	16
2.3 Preliminary Connection Design	16
2.4 Relevant Risks and Responses to Risks.....	16
2.5 Overall Risk Assessment Matrix.....	17
2.6 Risk Evaluation.....	18
3 Third Party Network Connection Examples	18
3.1 Private Leased Line.....	19
3.2 Site to Site VPN with DMZ.....	19
3.3 Traditional Site to Site VPN	19
3.4 Site to Site VPN Internal DMZ	20
3.5 VPN Client to Host Concentrator	20
3.6 Connection Diagrams	21
3.7 External Network Connection Policy Sample	26
4 Training and Awareness Sample Document	29
5 Connection Request Definitions	34
6 Frequently Asked Questions (FAQs)	35

Standard

This standard provides guidance to members of the American Petroleum Institute (API) for implementing secure third-party connections between the information technology systems and network of two companies that have a business relationship and a common objective.

The standard does not supplant or comment on the security procedures adopted by any individual company. The American Petroleum Institute does not perform the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees and others about security risks and precautions nor undertake their obligations under any laws.

API Companies recognize that effective security is a combination of layered security processes, policies, procedures, education, awareness, and assessments to ensure compliance. Companies use a variety of content filtering and audit programs to safeguard their systems in order to mitigate and minimize its vulnerabilities and risks.

API Companies, such as operators and oil-field suppliers, work closely on projects for long periods. These close relationships often require employees to work in the offices of another company or require access to data located in the other company's IT system. Yet, these employees also need access to their own employer's system. As a result, the protection of each company's system and data from unauthorized access or manipulation concerns the entire industry, causing security standards to become even more pressing.

API Companies have implemented enhanced IT security measures to provide security, such as the following:

- Reduction of: passing of sensitive information out of the company by employees, use of weak passwords, unauthorized access to facilities and networks, telephone fraud, spread of computer viruses, software piracy, and unauthorized electronic mail (email) or Internet usage.
- Increased electronic access control to facilities and networks by the use of badges, authentication services and proximity controls.
- Increased monitoring of intrusion detection systems.
- Endorsement of International Organization for Standardization (ISO)/IEC International Standard 17799, Information Technology—Code of Practice for Information Security Management. This standard covers the preservation of confidentiality, integrity, and availability of IT access, hardware, software, and data.

Trust

Method for Trust Establishment

The establishment of trust between companies with third-party connections requires that each company assume specific responsibilities and create a security plan.

Responsibilities

To establish trust in a third-party connection, each company must hold responsibility for its own internal security. The following is a guide for the companies to establishing security.

- Assess the potential risk to company operations and assets of a security breach through the third-party connection. The assessment determines the likelihood of a breach, type of breach, and consequences. The consequences include the potential risk to the financial stability of the company and effect on its customers (API Risk and Assessment Process).
- Develop a confidential security plan to safeguard the parts of the IT system at risk. The plan describes the potential risks and consequences, detection and deterrent measures taken to lessen the risks, and recovery from a security breach. The plan is reevaluated and updated periodically.
- Establish clear communication channels and responsibilities for assessing, preparing for, responding to and recovering from a security breach.

Companies in the third-party connection also agree to abide by this connectivity standard stating: all costs incurred are the responsibility of each company; The Company creating the connection(s) holds the liability; Connections can be terminated at any time.

Security Plan

An IT security plan should be an integral part of a company's overall security program. Each company considers to the extent possible its unique security risks and then assesses them to ensure the plan covers those risks. This standard recognizes the need for flexibility in the design of security plans and provides guidance for this need.

Some of the security plan must remain confidential. A confidentiality program can ensure understanding of what information can be shared and what remains confidential.

The ISO/IEC International Standard 17799 describes a framework for the creation of an IT security plan. This framework has been endorsed by API's Information Technology Security Forum as voluntary guidance to protect the oil and natural gas industry against acts of cyber terrorism. The standard attempts to ensure preservation of confidentiality, integrity, and availability of user access, hardware and software, and data.

The standard involves eight steps in the security process: Create an information security policy; Select and implement appropriate controls; Obtain upper management support; Perform security risk assessment; Create statement of applicability for all employees; Create information security management system; Educate and train staff; Audit.

Information on how to obtain this standard is provided at: <http://webstore.ansi.org/>.

1 Connection Request & Agreement Checklists

1.1 API Third Party External Network Connection Request Checklist

The following checklist includes items to consider collecting when creating a Third Party external network connection, including a general connection request document. Refer to the “Third Party External Network Connection Request Definitions” for further details on individual items:

- ☒ Parties involved in Third Party Network Connection Agreement
- ☒ Agreement contents/attachments
 - ☒ Agreement terms
 - ☒ [Third Party External Network Connection Detailed Request](#)
 - Technical Contact Information
 - Type of Network Connection
 - Risk Assessment
 - Risk Assessment Review
 - ☒ [Third party user responsibility Agreement](#)
 - *Property Definition*
 - *Property Rights*
 - *Acceptable Use*
 - *Monitoring*
- ☒ Modification requirements
- ☒ Dispute resolution
- ☒ Third Party authorized signatures
- ☒ Hosting Company authorized signatures

1.2 Third Party Connection Terms and Conditions Checklist

Agreement terms—Details the terms and conditions of the connection agreement including the objective of the agreement, a definition of the “network connection,” and connection terms.

The following checklist includes items to consider when developing a terms and conditions agreement:

- ☒ Network usage requirements
- ☒ Hosting company owned equipment guidelines for third party (e.g. Security policy, configuration/modification, software usage, physical security, facilities/equipment care, password requirements, and confidentiality)
- ☒ Network security (e.g. authorized use, third party leave, and Security policy/procedure maintenance)
- ☒ Notifications (e.g. user changes, functional changes)
- ☒ Payment of costs (e.g. cost separation and payment responsibility)
- ☒ Disclaimer of warranties
- ☒ Limitation of liabilities
- ☒ Confidentiality (e.g. disclosure guidelines, effective period, legal disclosure requirements)
- ☒ Term, termination and survival (e.g. agreement length, termination provisions including agreement breach, return of physical media and/or destruction of logical data)
- ☒ Miscellaneous (e.g. severability, waiver, assignment, force majeure, export control)

1.3 API External Network Connection Detailed Request Checklist

The following checklist includes items to consider collecting when creating a Third Party external network connection.

- ☒ Identify your external organization name and network information; including two (2) technical contacts, area code/telephone number, pagers email address, and location address.
- ☒ Identify the Hosting Company organization name and network that you will be accessing, including a technical contact, area code/telephone number, and location address.
- ☒ Indicate the type of connection requested either dial-up, dedicated private leased line or VPN (i.e. Site-to-Site VPN with DMZ, Traditional Site-to-Site VPN, or Site-to-Site VPN internal DMZ), see attachment 1—Guidance for Use Document for details related to the type of VPN required.
- ☒ Indicate the date the connection is required.
- ☒ Indicate the date the connection is to be terminated. (Elevated access should be limited and reviewed under tighter controls)
- ☒ Provide a technical description of the project, including assessment of current security level of external party. Include VISIO diagrams, risk assessment, and additional security controls that are to be implemented.
- ☒ Provide justification for the project, including alternatives considered.

1.4 API Third Party User Responsibility Sample Agreement

This agreement sets forth <Hosting Company>'s position confirming its right to protect <Hosting Company> property and that its contractors, consultants, and vendor's hereafter referred to as "Trusted Third Party" properly uses such property. Obligations and conditions set forward in this statement shall be in addition to any obligations, conditions, or commitments contained in any agreement(s) under or through which Trusted Third Party users are providing services to <Hosting Company>. The purpose of this agreement is to ensure that all <HOSTING COMPANY> users use <HOSTING COMPANY> computing facilities in an effective, efficient, ethical and lawful manner.

<Hosting Company> Property Defined—<Hosting Company> property is defined as, but not limited to, the following:

- a. All data, documents, correspondence, and intellectual property whether contained in electronic, physical, hard copy or other form, access cards, badges and keys to facilities, desks, and cabinets;
- b. Hardware, such as network resources including servers, PC's, workstations, networks, monitors, scanners, printers, telephones and voice mail, facsimile machines, cellular phones, pagers, secured id tokens, smart cards, and personal digital assistants;
- c. All User ID's, system/application/screensaver passwords, software, including all administrative office, e-mail, Internet, operating systems/applications, development applications or special tools and utilities supplied by the company;
- d. Work areas or related accessible areas, including desks or other workstations, drawers, supplies, and all storage areas.

I. Use of <Hosting Company> Property—As a Trusted Third Party you agree to observe and abide by the following with respect to <Hosting Company> property. For business purposes, you may be provided with a telephone, computer or workstation with network access to other resources or you may be authorized as a Trusted Third Party to connect your company's notebook to <Hosting Company>'s network. In either case you are responsible for the appropriate use of all property within or connected to <Hosting Company>'s domain and abiding by the following:

- a. Computer and communication systems may not be used to view, store, transmit or communicate any language or message that is perceived to be offensive or threatening on the basis of race, sex, religion, age, national origin, political orientation, disability or any other basis. Company policies prohibit the transmission of vulgar, pornographic, obscene or threatening messages.
- b. <Trusted Third Party> may use <HOSTING COMPANY> computing systems and facilities for only lawful purposes. Transmission, distribution or storage of material in violation of any applicable law or regulation is prohibited. This include, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, fraudulent, harassing, constitutes an illegal threat, or violates export laws.