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.

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

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.

c. <Trusted Third Party> shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized <HOSTING COMPANY> user access to a <HOSTING COMPANY> resource; obtain extra resources, beyond those allocated; circumvent <HOSTING COMPANY> computer security measures or gain access to a <HOSTING COMPANY> system for which proper authorization has not been given.

d. <Trusted Third Party> is requested to report any weaknesses in <HOSTING COMPANY> computer security, any incidents of possible misuse or violation of this agreement to the proper authorities at <HOSTING COMPANY>.

e. The presence or use of techniques or vulnerability assessment and discovery tools such as scanners and sniffers that are capable of hacking against <Hosting Company>'s network or launch attacks against others from within <Hosting Company>' network is strictly prohibited. <Trusted Third Party> shall not download, install or run any such security programs or utilities.

f. The telephone system and all communications transmitted by, or stored in this system, are the property of <Hosting Company>. This includes the use of telephones, voice mail, fax machines and modems. Personal use of the telephone should be limited and all long distance telephone calls not related to Company business should be billed to your personal calling account. <Trusted Third Party> shall not divulge <Hosting Company> modem phone numbers to anyone outside of the organization.

g. Computer hardware and software should not be removed from Company premises without prior management approval.

h. Copyright laws prohibit making copies of licensed computer software unless it is specifically permitted within a licensing agreement. Violations may place <Hosting Company>, you and your company at legal risk.

i. Company computers and workstations should only have <Hosting Company> approved software installed on them. Personal software or non-<Hosting Company> licensed software should not be installed on any workstation.

j. The presence and/or release of malicious code (Trojan's, viruses, worms etc.) capable of causing damage or harm against or within <Hosting Company>'s networks is strictly prohibited.

k. Software developed by a Trusted Third Party using <Hosting Company> systems shall be considered the sole property of <Hosting Company>.

l. Trusted Third Party users are provided password-protected user accounts for computer system access. Passwords should not be shared with fellow employees. <Trusted Third Party> is responsible for protecting any information used and/or stored on/in their <HOSTING COMPANY> accounts.

m. Electronic mail messages are considered discoverable in a legal proceeding. Trusted Third Party users should exercise the same caution with electronic data as they would with paper documents.

n. Sensitive or confidential information should not be sent by electronic mail. Special security and communication software is available to encrypt sensitive data. When using electronic mail, there should be no expectation of privacy.

o. Inappropriate non-business uses of the Company's Internet and electronic mail systems are prohibited. This includes but is not limited to using systems to access or transmit sexually explicit material, offensive jokes, chain letters, product solicitations, personal mass mailings or conducting a personal business. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on <HOSTING COMPANY> systems. <Hosting Company> considers the information that people generate, document and communicate using <Hosting Company> computer resources to be <Hosting Company>'s property. <Hosting Company> reserves the right to monitor, inspect, review, or retain any electronic mail or computer records on <Hosting Company> computer resources.

p. All inbound and outbound electronic transmissions, including information obtained via the Internet, are considered the sole property of <Hosting Company>. The Company exercises its right to scan and monitor all computer and communications systems use (including inbound and outbound electronic mail transmissions, file transfers and Internet usage). When using <Hosting Company>'s systems users expressly accept and consent to having their activities monitored.

q. Information protected by confidentiality agreements, nondisclosure agreements, licensing agreements, or copyright law should not be posted on publicly accessible bulletin boards, chat rooms or Internet sites.

r. <Trusted Third Party> shall not attempt to access any data or programs contained on <HOSTING COMPANY> systems for which they do not have authorization or explicit consent of the owner of the data/program.

s. Activities designed to circumvent, compromise or otherwise exploit computer security controls are prohibited.

t. Access to any <Hosting Company> network by Virtual Private Network (VPN) is exclusively for use in the performance of <Hosting Company> business, and users will not share it or the system privileges that it provides with any other person.

II. Monitoring—<Hosting Company> reserves the right to scan, monitor and inspect any and all computer systems to include hard disks, media, inbound/outbound email and Internet traffic) for malicious or inappropriate content or attachments in accordance with the company's monitoring standards and procedures. Authorized personnel routinely monitor <Hosting Company>'s network and systems for performance, maintenance and unauthorized activity. All individuals who access and use <Hosting Company> resources are subject to having their activities monitored and recorded. Information and material assets that reveal unauthorized or improper use of <Hosting Company> resources by an employee, contractor, consultant, vendor or service provider will be retained and used as evidence to support disciplinary action and/or criminal prosecution. All individuals using <Hosting Company> systems expressly consent to such scanning, monitoring or inspection and agree not to use the company's systems in violation of company policy. A violation of this agreement subjects the undersigned to action up to and including termination and/or criminal prosecution.

Any noncompliance with this agreement will constitute a security violation and will be reported to the management of the <Trusted Third Party> user and may result in disciplinary action, including termination. Serious violations may result in civil or criminal prosecution.

I acknowledge that I have been briefed and have read the information in this Acknowledgment. I understand my responsibilities regarding the use and protection of <Hosting Company> Property and consent to the scanning, monitoring and inspection of resources and my use of <Hosting Company> property. Upon my resignation or contract termination from <Hosting Company>, I will return all <Hosting Company> Property in my possession and disclose all system/application/screensaver passwords.

Name: _____

Signature: _____ *Date:* _____

Telephone: _____

1.5 External Network Connection Information Sample Request Form

Section I: Request Information

Date	
Requestor Name	
External Organization Name	
Technical Contact 1	
Phone/Pager/Email Address	
Location Address	
Technical Contact 2	
Phone/Pager/Email Address	
Location Address	
<Hosting Company> Organization Name	
Technical Contact	
Area/Telephone Number	
Location Address	
Business Unit Information Security Coordinator	
Type of Connection Requested	o Dial-Up o Dedicated o VPN **6.1.1.1 VPN Options** o Site-to-Site VPN with DMZ o Traditional Site-to-Site VPN o Site-to-Site VPN internal DMZ o VPN client to host concentrator
Date Connection Required	
Date Connection to be Terminated	

Technical Description: **(Failure to include this information will result in a delay in approval**)

Required Attachments include:

1. Network Diagram (Prefer Visio)
2. Risk Assessment
3. Additional Security Controls
    a. Hardening of servers
    b. Router or switch access controls
    c. New Firewall rules
    d. Services required (include IP addresses & open ports required)

Other:

1. What applications will be used?
2. Bandwidth requirements?
3. What types of data transfer will be done?
4. What are the estimated hours of use each week? What are the peek hours?
5. How many external employees will use this connection? (List names & telephone numbers).
6. What is the location of the termination point of this network connection?
7. Identify all <Hosting Company> owned equipment maintained at the Third Party Site.

Business Justification: (Use additional pages if needed.)

Section I: Approvals

Restrictions: (Initial your comments for reference identification. Any party, including the Requester, may enter comments or instructions to restrict or control access.)		
Network Architecture Representative	Signature:	Date:
Information Security Representative	Signature:	Date:
Business Manager/Resource Owner	Signature:	Date:
Implementation Date		

2 Risk Analysis Template

Document Purpose

The purpose of this document is to record the connection risks associated with third party connectivity to the <Hosting Company> network. Prior to development of this document, the Data, System and Application Owners must provide their risk information to the <Hosting Company> Information Security Manager or applicable person.

2.1 Executive Summary

2.1.1 Sponsor

2.1.2 Third Party

2.1.3 Description of the Business Need for this connection

2.2 General Connection Information

2.2.1 Data, System and Application Owners

2.2.2 Data Owner(s)

2.2.3 System Owner(s)

2.2.4 Application Owner(s)

2.3 Preliminary Connection Design

2.3.1 Connection Method

{Identify the approved technical solution (e.g. Citrix, VPN, frame relay) that will support the connection of the third party into the <Hosting Company> network.}

2.3.2 Computing Resources to Be Accessed

2.3.3Network Access Authorization

{Describe the process for granting access to IT resources.}

2.3.4 Network Access User Authentication Level

{Describe the required level of user authentication based on the Security Classification and input from the Data, System and Application Owners. In the cases of one or two factor authentication, describe where authentication will take place.}

2.3.5 Forced Path Description

{Describe the controls to be implemented (i.e., the forced pathway to be traversed among information technology assets) to route the third party from their entry into the <Hosting Company> network to their requested destination. The description must identify the degree to which a forced path can be established. For example, describe whether the path will be forced to the device (IP address) or to the application (IP address and TCP port number).}

2.4 Relevant Risks and Responses to Risks

2.4.1 Risk Identification

{This section contains the descriptive (non-quantitative) risk information.}

2.4.2 Data Risks

{E.g. how is data classification managed; what logical access controls are in place; is encryption used to protect sensitive data; etc.}

2.4.3 System Risks

{E.g. what monitoring tools are in place to detect intrusion attempts; how often are logs reviewed; is there a formal approval process for all external connections; etc.}

2.4.4 Application Risks

{E.g. how is application data integrity ensured; etc.}

2.4.5 Connectivity Risks

{List any unusual connectivity related risks identified by the IT Security Group.}

2.4.5 Risk Response Development

{Given the (1) the preliminary connection design and (2) the risks described above, describe any additional controls that may be recommended to avoid or further mitigate the risks.}

2.5 Overall Risk Assessment Matrix

{Identify and document the overall assessment of the risk (Low, Medium, or High) for this third party connection.}

Risk Matrix

Likelihood \ Business Impact	Lo	Mediu	Hig
Hig	3	1	1
Mediu	3	2	1
Lo	4	3	2

Definition of Likelihood (Includes implementation of noted 'controls in place')

- High Likelihood: Certain or almost certain to occur during the lifetime of the asset or activity
- Medium Likelihood: Might occur during the lifetime of the asset or activity
- Low Likelihood: Unlikely to occur during the lifetime of the asset or activity

Definition of Business Impact

- High Impact: Significant business loss will result
- Medium Impact: Moderate business loss may result causing disruption to business, however recovery is possible
- Low Impact: Distracting to business, however recovery can be made with no long-term impact

Priority Actions

- Priority 1 – Effective countermeasures must be implemented
- Priority 2 – Firm action plans must be developed
- Priority 3 – Should be monitored for impact
- Priority 4 – Requires no action at present

2.6. Risk Evaluation

2.6.1 Overall Risk Evaluation

☐ High

☐ Medium

☐ Low

2.6.2 Connection Recommendation

☐ Approve the connection as described in the preliminary design.

☐ Approve the connection with the additional controls described in this document.

☐ Disapprove the Connection.

Acceptance of risk by IT Security Manager

I hereby approve the risk as specified on the attached risk assessment:

Name (Name, Company)	Date	Approved (Signature)

Acceptance of risk by Business Manager

I hereby approve the risk as specified on the attached risk assessment:

Name (Name, Company)	Date	Approved (Signature)

3 Guidance for use—Third Party Network Connection Examples

Third Party Network Connection Examples

- **Option 1: Private Leased Line**
- **Option 2: Site to Site VPN with DMZ**
- **Option 3: Traditional Site to Site VPN**
- **Option 4: Site to Site VPN—Internal DMZ**
- **Option 5: VPN Client to Host Concentrator**

3.1 Option 1—Private Leased Line

- Use if:
  - 1st choice if cost and network availability is not an issue
  - High service level required (SLA)
- Pros:
  - Most Secure
  - Private circuit PIP, Frame Relay, ISDN, etc.
  - Data is not transmitted across the Internet
- Cons:
  - Reliability—Redundancy expensive
  - Availability—Dependent on service provider
  - Still may require firewalls
  - VPN may or may not be a requirement depending on the sensitivity of the data
  - Service providers could tap into data streams if unencrypted
    - Risk is low due to private circuit (typically frame relay or pip cloud)
  - Cost is high—increases as the distance between offices increases

3.2 Option 2—Site-to-Site VPN with DMZ

- Use If:
  - System can be relocated to the DMZ & private lease line is not an option
- Pros:
  - No internal network connectivity is required
  - Uses existing Internet Firewall & controls
- Cons:
  - Systems in the DMZ must be stand alone systems (no domain authentication)
  - Less Secure than a private leased line due to exposure to Internet
  - Systems on the DMZ are exposed to the Internet and other systems in the same DMZ

3.3 Option 3—Traditional Site-to-Site VPN

- Use if:
  - System cannot be moved to DMZ
  - Protocols, Ports, services and IPs required are very restrictive and do not permit "**jumping off**"
  - Internal Firewall is not available and you do not want encrypted tunnels across your internal network
- Pros:
  - Simple configuration and setup
  - Uses existing Internet Firewall & controls
- Cons:
  - Encryption ends at perimeter Firewall – risk of password sent in the clear being captured over Internal network
  - Access list on end switch or router required for restricting access to end network device (less secure than Firewall)

3.4 Option 4—Site to Site VPN—Internal DMZ

- Use If:
  - System cannot be moved to the DMZ
  - "Jumping off" protocols or services are required (Telnet, Remote Control, etc)
- Pros:
  - More Secure than VPN Site-to-Site
- Cons:
  - Requires an additional Firewall and controls on the Internal network
  - Traffic transmitted over VPN is encrypted over internal network
  - IPSEC/HA must be routed over your internal network

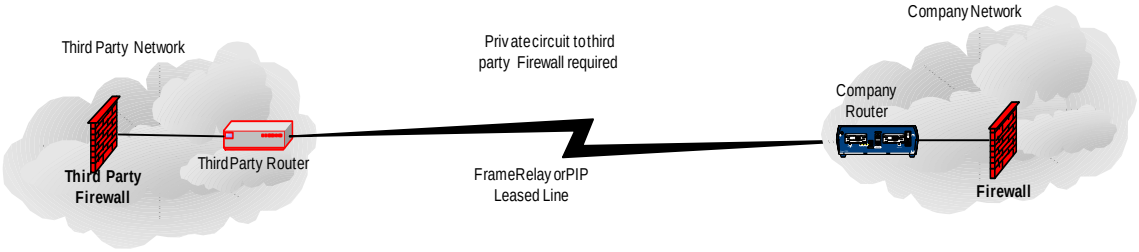
3.5 Option 5—VPN Client to Host Concentrator

- Use If:
  - Use when very restrictive policies can be implemented for filtering by source and destination IP addresses & port
  - "Jumping off" protocols or services are not required (Telnet, Remote Control, etc)
- Pros:
  - Configuration is simple
  - Cost is minimal, VPN client and two-factor authentication (SecureID or certificate) required
- Cons:
  - May require a company computer if unlimited access to the network is required
  - Traffic transmitted over internal network is unencrypted
  - Potential for external party systems to infect local systems if not properly protected

3.6 Diagram Samples

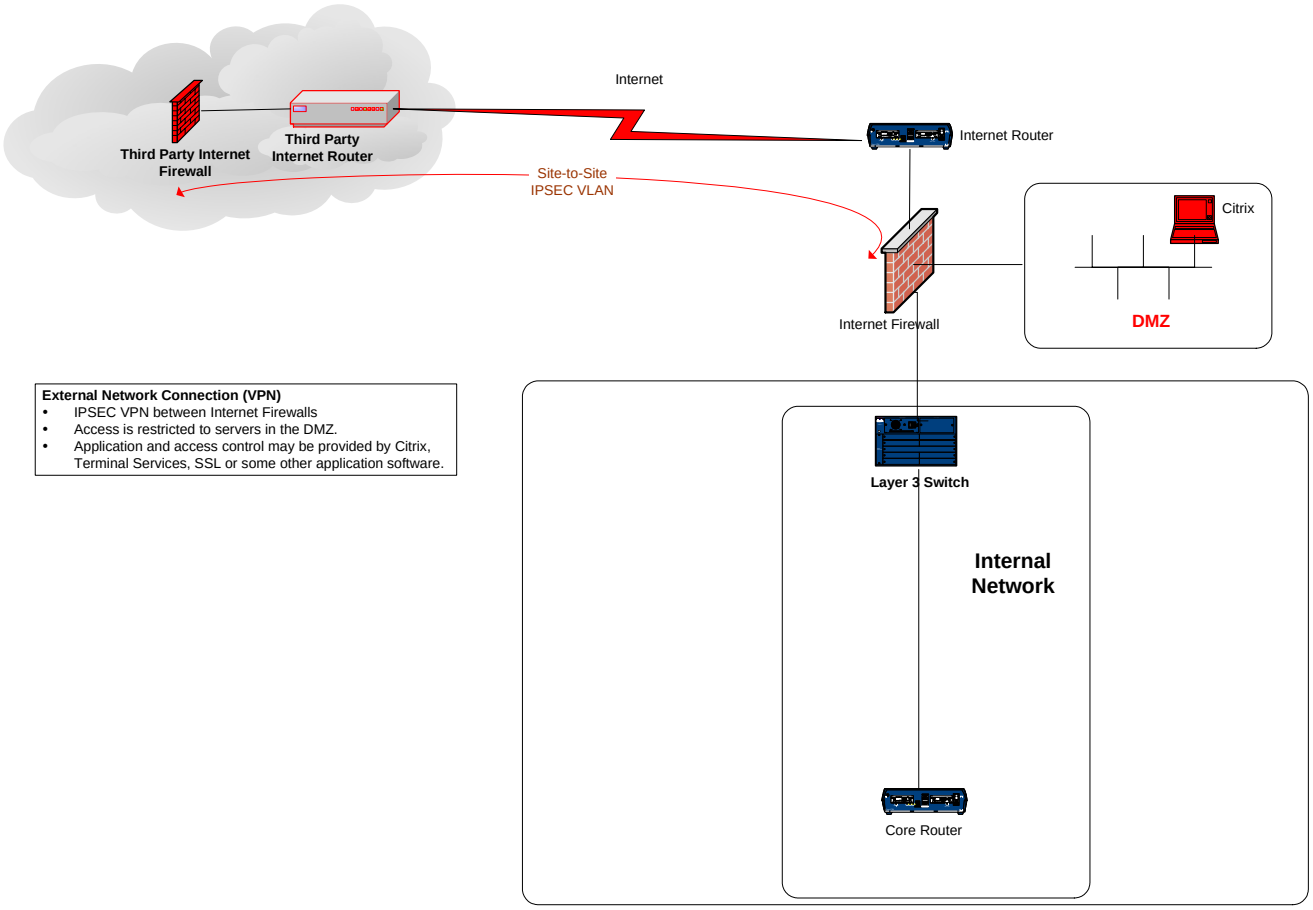
Option 1—Private Leased Line Diagrams

API Third Party External Network Connection - Private Leased Line



Option 2—Site to Site VPN with DMZ

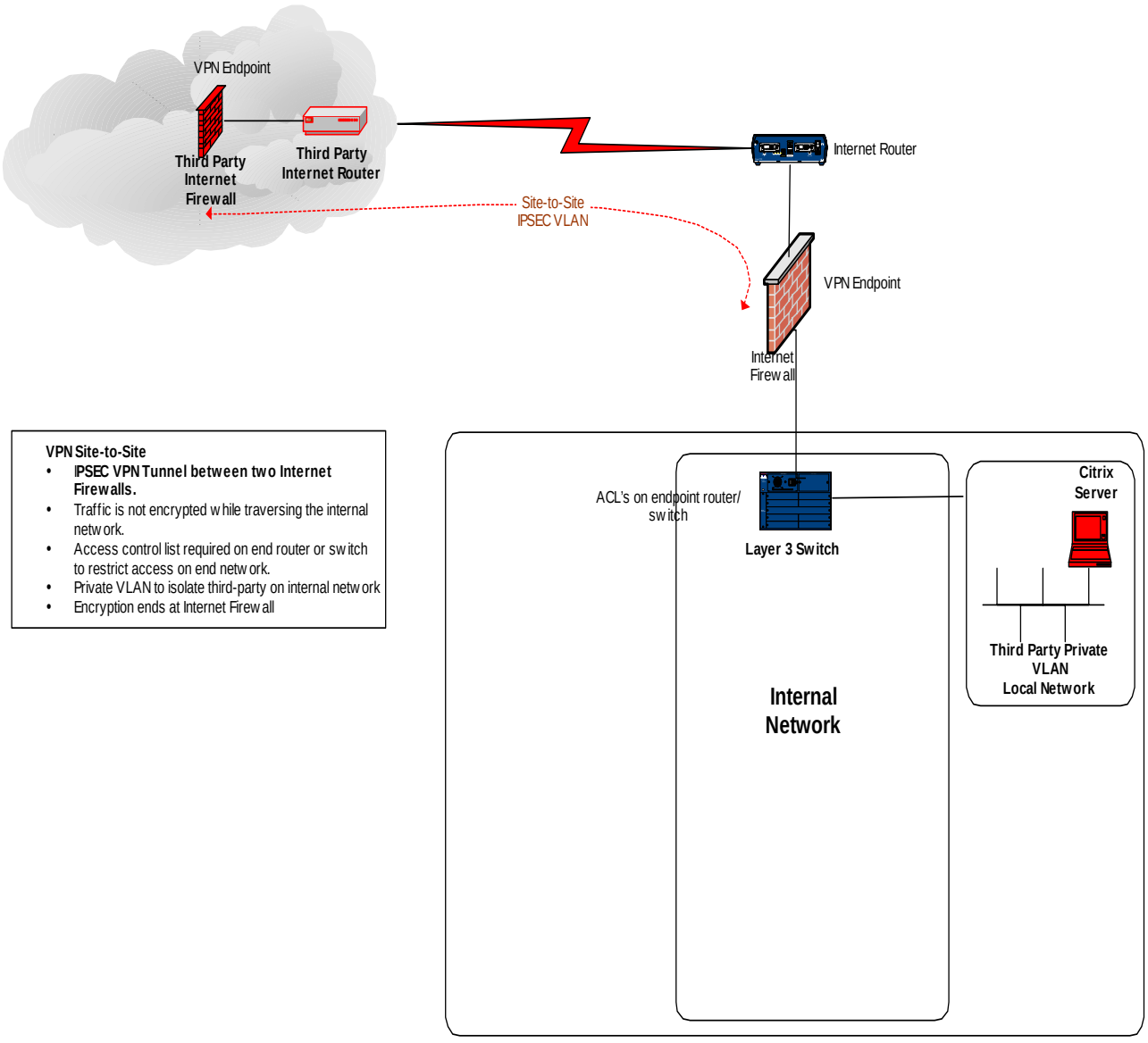
API Third Party External Network Connection - DMZ



External Network Connection (VPN)
- IPSEC VPN between Internet Firewalls
- Access is restricted to servers in the DMZ.
- Application and access control may be provided by Citrix, Terminal Services, SSL or some other application software.

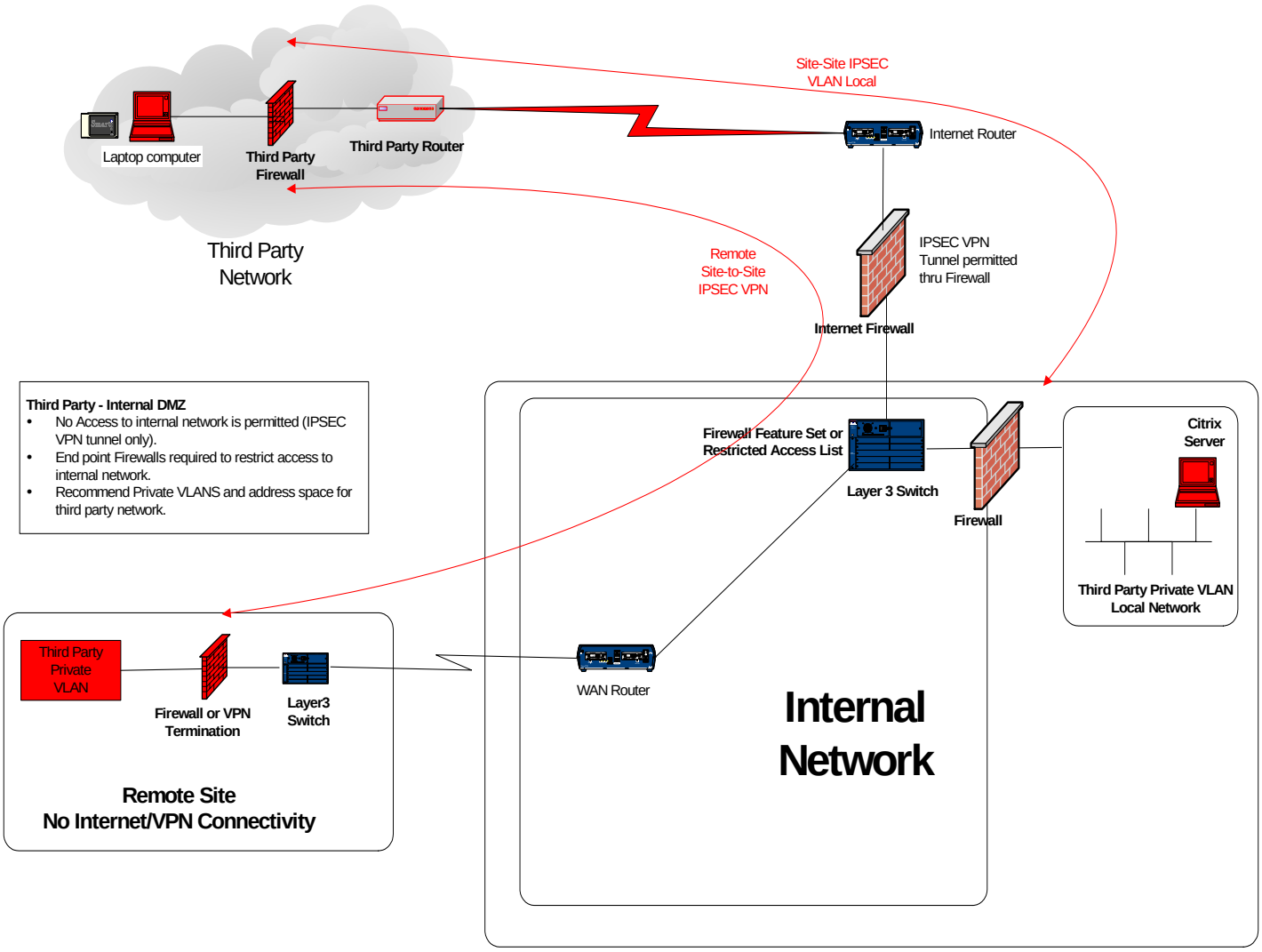
Option 3—Traditional Site to Site VPN

API Third Party External Network Connection - VPN Site-to-Site

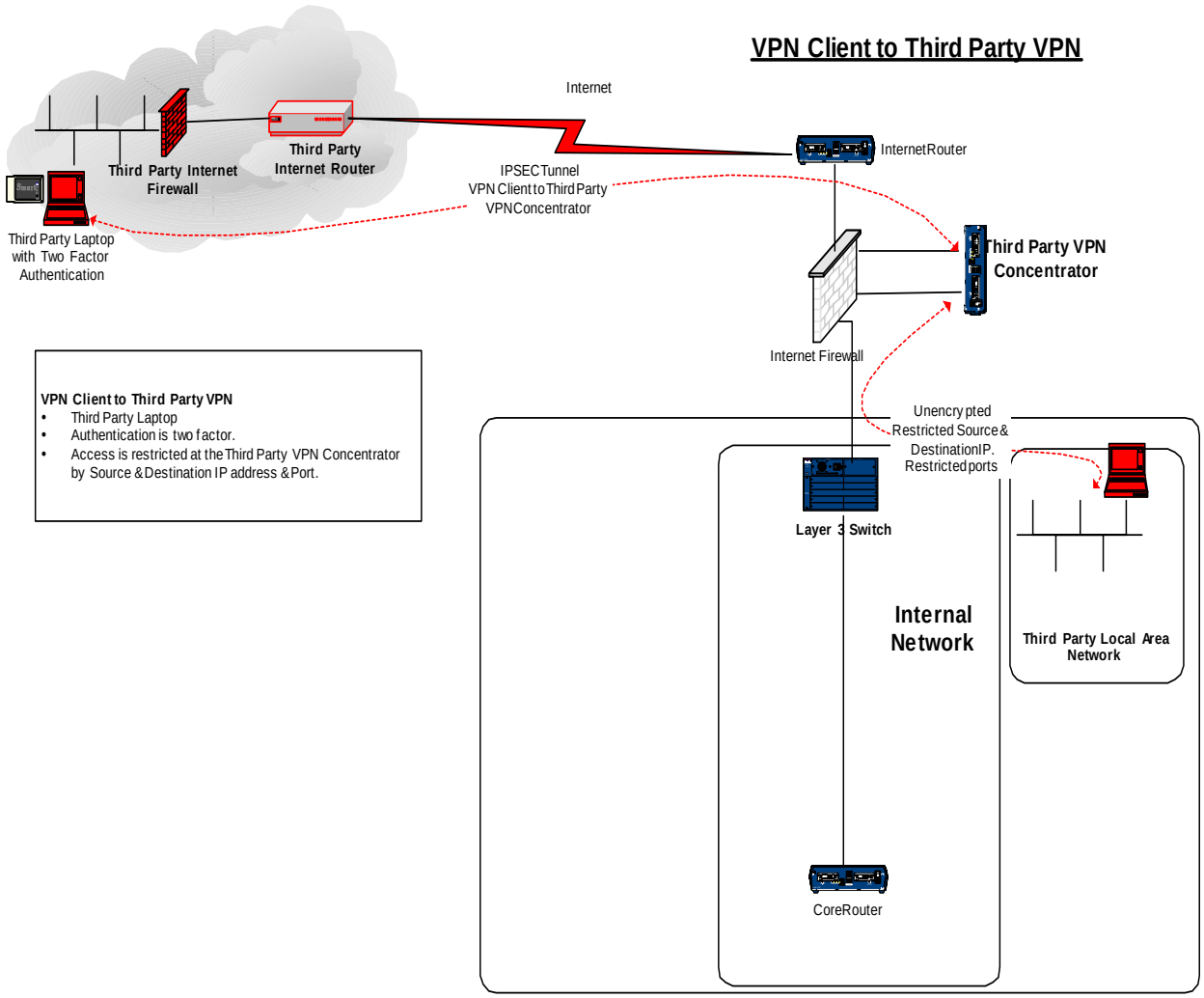


Option 4: Site to Site VPN—Internal DMZ

API Third Party External Network Connection - Internal DMZ



Option 5—VPN Client to Host Concentrator



3.7 External Network Connection Sample Policy

NETWORK CONNECTION POLICY

Purpose: To ensure that a secure method of network connectivity between <Hosting Company> and all third parties and to provide a formalized method for the request, approval and tracking of such connections.

Scope: External third party network connections to <Hosting Company> can create potential security exposures if not administered and managed correctly and consistently. These exposures may include but are not limited to unapproved third party network connections to the <Hosting Company> network, the inability to shut down access in the event of a security breach, exposure to hacking attempts, and the spread of worms or malware across the third party network connection. Therefore, all external third party network connections (dial-up, dedicated or VPN, or Contractor VPN Client) must be certified and approved by <designated representative> prior to implementation. This policy applies to all new Third Party Network Connection requests.

Definitions:

A "Network Connection" is defined as one of the connectivity options listed in Section B below. Third Parties are defined as <Hosting Company> Partners, Vendors, Suppliers, etc.

A. Third-Party Connection Requests and Approvals

All requests for Third Party Network connections must be made using the appropriate methods as specified in **Third Party Network Connection Request** document. The Third Party Network Connection Request document requires the following <Hosting Company> documents to be completed and authorized by the appropriate individuals prior to connecting any external third party networks to the <Hosting Company> network.

1. API Third Party External Network Connection Request
2. API Third Party Connection Agreement Terms and Conditions
3. API Third Party External Network Connection Information Request
4. API Third Party User Responsibility Agreement

B. Connectivity Options

The connectivity options below are the standard methods of providing a Third Party Network Connection. The type of connection established is at the discretion of <Hosting Company>. Requests to deviate from these standard methods must be accompanied by a <Hosting Company> Information Security Standards Exception request form and approved by the <Hosting Company> Information Security Manager.

- **Option 1: Private Leased Line**
- **Option 2: Site to Site VPN with DMZ**
- **Option 3: Traditional Site to Site VPN**
- **Option 4: Site to Site VPN—Internal DMZ**
- **Option 5: VPN Client to Host Concentrator**

C. Services Provided

In general, services provided over <Third Party> Network Connections should be limited only to those services needed, and only to those devices (hosts, routers, etc.) needed, as defined in the External Network Connection Request Form. **Blanket access will not be provided for anyone.** The default policy position is to deny all access and only permit those specific services that are needed and approved by <Hosting Company> pursuant to the established procedure.

In no case shall a Third Party Network Connection to <Hosting Company> be used as an Internet connection for the <Third Party>.

D. Authentication for Third Party Network Connections

<Third Party> Network Connections made via VPN connections over the Internet will be authenticated using the <Hosting Company> Two Factor Authentication. Exceptions to this will be documented in the External Network Connection Request Form.

E. <Hosting Company> Equipment at <Third Party> Sites

In many cases it may be necessary to have <Hosting Company>-owned and maintained equipment at a <Third Party> site. All such equipment will be documented on the **<Hosting Company> External Network Connection Information Request** document. Access to <Hosting Company> network devices such as routers and switches will only is provided to <Hosting Company> support personnel. All <Hosting Company>-Owned Equipment located at <Third Party> sites must be used only for business purposes. Any misuse of access or tampering with <Hosting Company>- hardware or software, except as authorized in writing by <Hosting Company> IT Security Manager, may, in <Hosting Company>'s sole discretion, result in termination of the connection agreement with the <Third Party>.

F. Protection of <Third Party> Private Information and Resources

The <Hosting Company> network support group responsible for the installation and configuration of a specific <Third Party> Network Connection must ensure that all possible measures have been taken to protect the integrity and privacy of <Hosting Company> sensitive information. At no time should <Hosting Company> rely solely on access/authorization control mechanisms at the <Third Party>'s site to protect or prohibit access to <Hosting Company> confidential information.

<Hosting Company> shall not have any responsibility for ensuring the protection of <Third Party> information. The <Third Party> shall be entirely responsible for providing the appropriate security measures to ensure protection of their private internal network and information.

G. Virus Program Contamination

<Hosting Company> and the <Third Party> shall take all reasonable measures to prevent the introduction into and propagation of Viruses by, (i) any of the equipment at their respective locations and (ii) their respective networks. <Hosting Company> and the <Third Party> shall check all computer software files and computer data files to be provided to the other immediately prior to delivery to ensure that they are free from Viruses.

If one party ("the first party") discovers a Virus at its location or on its network which has affected or which could affect the equipment or networks of the other party, then the first party shall immediately notify the other party that a Virus has been detected giving details about the nature of the Virus in question.

H. Audit and Review of <Third Party> Network Connections

All aspects of <Third Party> Network Connections - up to, but not including <Third Party>'s firewall, will be monitored by the appropriate <Hosting Company> network support group. Where possible, automated tools will be used to accomplish the auditing tasks. <Hosting Company> is responsible for monitoring access reports.

All <Third Party> Network Connections will be reviewed on an annual basis and information regarding specific <Third Party> network connections will be updated as necessary. Obsolete/non-compliant <Third Party> network connections will be terminated.

4 Training and Awareness Sample Document

As a trusted <Third Party> you have been entrusted with information of <Hosting Company>. That trust carries a responsibility and an obligation by you to ensure that information of <company name> is used only for its intended business purpose. This section describes why information security is important and what you need to know to be an active participant in <company name> information security program. You will be required to review and understand <company name> information security policies and sign a User Acknowledgment Statement, which is an acceptance of understanding and acceptance of responsibility.

To understand why there's an information security program we must define what information is, why it's important and what the security program is all about.

Information is one of the company's most valuable assets and need to be protected from loss, unauthorized changes and disclosure. Information appears in many forms:

- Personal computer records
- Word processing, spreadsheets and graphics documents
- Letters and memos
- Paper reports
- Magnetic media
- Conversation

Why should the user be concerned about information security?

Information accessed by the user every day must be protected. Whether the user works with paper records or a terminal, or spends most of the day on the phone, the user is the protection link between the company's information and information security program.

Why is the user important?

By preventing errors, security makes the user's job easier because they won't have to spend time fixing mistakes. Good security helps to keep the company healthy by ensuring that the information is available and protected.

Why are information security controls important?

Controls are needed to make sure each person is accountable for his or her own actions. Controls protect the honest user from unwarranted suspicion. Without accountability, all are equally suspect when something bad happens.

Honest errors or omissions usually cause problems with information. Controls help identify those who need help and limit the damage their mistakes can cause.

What could happen without controls?

Information is an asset and the loss of information can cost time and money. Information that is incorrect can lead to all kinds of trouble. Here are a few of the things, which could result from poor security:

- Information could be lost costing the company money to recreate that information.
- Inaccurate information could be sent to a client causing the company to lose that client.
- Management could make a bad decision based upon incorrect information.
- Giving out private information could cause a client embarrassment. As a result, the company might lose the client or even be sued.
- A rival might obtain company information causing the company to lose a competitive advantage.

Are there legal reasons for protecting my company's information?

There are federal and state laws, which make people legally responsible to be sure information is correct and used appropriately. The laws:

- Protect a person's right to privacy.
- Prohibit violations of copyrights, patents and trade secrets.
- Prohibit unauthorized computer access.

How can a user protect the information in their work area?

People become careless about the information in their work area because everyone has access to it. But it's important to prevent access by unauthorized visitors:

- Lock sensitive documents in a cabinet or drawer.
- Clear desks of all papers at the end of the day.
- Keep keys hidden.
- Don't discuss sensitive information in areas where it can be overheard.
- Establish a need to know before discussing information with other workers.
- Label sensitive documents appropriately.
- Challenge unauthorized visitors.

Are some visitors OK?

Yes, but that doesn't mean they should be allowed to see information. Anyone external to a department or company is a visitor. Use caution when disclosing information in front of any visitor. This includes:

- former employees of your company
- sales people, and
- clients or customers

How do I handle questions from outside people?

You may come into contact with a number of outside people from time to time. How you handle them depends upon who they are. Here are some suggestions:

- Refer any requests from the media (reporters) to the appropriate people in your company. This may be a department in charge of public relations or senior managers.
- When asked to complete a survey or questionnaire, ask your supervisor whether this is all right.

– If you receive calls from employment search companies or vendors, take the individual's name and number and pass this along to the appropriate person. Do not allow such people to have a copy of your company's list of employees or telephone book. This would allow them to make calls that others in your company may not welcome.

How do I handle suspicious phone calls?

When speaking on the phone, you could easily be fooled into thinking you are talking to a person with a real need for some facts. Be careful not to give out valuable information to the wrong person. This is known as Social Engineering. Here are some points to remember:

– Verify the identity of the caller. If you can't do this by asking some key question, then tell the caller, "I will need to call you back on this."
– Verify the caller's need to know the requested information.
– Be careful not to give out unnecessary information.
– Be aware of who is in the area and who could overhear your conversation.

How do I dispose of sensitive information or documents?

Check with your manager or supervisor about the approved method for disposing of trash. Some of the methods that may be used include:

– Shred the document. Remember that reports are very readable if you shred them so the lines of print can still be read! Shred reports down the page instead of across. With microfiche, you can feed the documents in at an angle.
– If your office has such a program, place the document in a special collection bin for sensitive trash. Someone else will collect it and make sure it gets shredded.
– Some companies specialize in the disposal of sensitive trash. Check the phone book and call someone to come pick up your trash and shred it. If it is extremely sensitive, you may want to go along and watch it being shredded.
– When getting rid of worn out floppy diskettes that have sensitive information on them, cut them in half before putting them in the trash.
– If you pass a diskette or other electronic media along to someone else, reformat it first. Just deleting information does not mean that the information has been erased. If the diskette contains highly sensitive data, it should never be passed along. There will be some data that can be read even after you have reformatted the diskette.

The workstation is important too!

Here are some of the things you can do to protect it:

– Make sure that anyone you see using a workstation in your area is authorized to do so.
– When sensitive information is on the screen, be sure no one else can see it.
– Be sure to sign off when you leave your workstation, even if you plan to return in a few minutes.
– Protect your password.

Why is password protection important?

Your password gives access and is for your personal use. You are responsible for any access made under your userID and password. Anyone with a password should protect it. Protect your password with the following smart practices:

- Change your password periodically.
- Change your password immediately if it becomes known to others.
- Choose hard to guess passwords.
- Enter your password in private.
- Log off the terminal after each usage.

Provide guidance on your company's password policy and suggestions on how to select good passwords. The whole idea of a password is to keep someone else from using your userID. Some passwords are easy to guess, especially if the other person knows you.

Here are some passwords to AVOID:

- Your name, nickname, initials
- Your user identification code
- Dates, especially those that appear on your driver's license, in a calendar you carry in your purse or wallet
- Consecutive keys on a keyboard, e.g. QWERTY or FGHJKL
- Repeated characters, e.g. CCCCCC or 9999999
- Your telephone number, employee number, social security number
- Dictionary words.

Here are some suggestions for choosing a GOOD password:

- Combine letters and numbers such as the name and birth date of a relative or friend, e.g. LISA105.
- Take the first or last letters from each word of a phrase, e.g. 1WADASN (It Was A Dark And Stormy Night) or EDESOEFT (wE holD thesE truthS t0 bE se1F evidenT).
- Remove all vowels from a common word or words, e.g. TPSCRT (ToP SeCROT).
- Make it as long as possible.

Just a reminder, DON'T use any of our examples! A lot of people will be reading this handbook!

How do I protect my information at home?

The same rules apply at both work and home. Make sure you know the classification of the information and the appropriate controls. Be sure that you:

- Lock up information when it is not in use.
- Make backup copies and protect them the same as the originals.
- Protect the information from damage and destruction.
- Protect sensitive information from casual observation by others.

Bringing personal computers from home to the office

This is not recommended. Many companies have policies forbidding this. If you are allowed to do so, remember:

- Company insurance policies probably won't cover the equipment if anything happens to it.
- If the equipment is stolen, your company generally won't replace it.
- Although the computer is yours, the information on it belongs to your company and must be protected as usual.

Can I copy company-owned software to home computers?

That depends on the software. Misuse of privately owned software can expose your company and you to lawsuits, so get expert advice before you do anything. When in doubt, don't copy! Here are some guidelines for copying software:

- Get your managers approval before copying any software.
- Although you may have purchased the software, what you' really buy with most packages is a license to use the software on one machine.
- Unauthorized copying of software is a violation of the U.S. Copyright Law. It is critical that you check the terms of your license to make sure you are not violating the agreement with the vendor.
- Some agreements with software vendors may allow copying if the work is business related. Check with your manager to see if this applies.
- You may need to register your use of the software with the vendor.
- If you are borrowing the original diskette, use great care to protect the diskette from damage.

Can I copy software I write?

Depends on your company's policies about use of company software. Software you write belongs to your company if:

- You use company equipment to develop it.
- You develop it on behalf of your company.
- You develop it on company time regardless of what equipment you use.
- Some companies' policies state that as long as you work for them, anything you develop belongs to your company.

What are appropriate backup procedures?

Remember that the purpose of an extra copy is to replace the main copy if something happens to the first copy. Here are some important points to remember:

- Make an extra copy of the information for safety. If you have the information on a diskette and on paper, it is usually easier to copy the diskette.
- Make an extra copy of the information whenever it has been changed enough to require a fresh copy. For some information, you may need to make a new copy every day or even every hour.
- You may want to send your extra copy out of your building as a protection against an office fire. If you regularly exchange information with another office, you might want to ask them to store reports or diskettes for you too.
- In special cases, make two extra copies: one to keep in your office and one to send out of the building.
- If the original becomes damaged, make a new backup from the first backup before using.

5 Connection Request Definitions

Agreement contents/attachments—This should include a list of all agreements requiring approval/signature between the hosting company and third party, including the general Third Party External Network Connection Request as well as:

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. Terms may include:

- 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, confidentiality)
- Network security (e.g. authorized use, third party leave, 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 beach, return of physical media and/or destruction of logical data)
- Miscellaneous (e.g. severability, waiver, assignment, force majeure, export control)

Dispute resolution—Any disputes arising out of or in connection with the Agreement shall be governed by applicable state law without regard to choice of law provisions. Prior oral and written communications outside of the document are void.

Frequently Asked Questions

1. *What ports must be permitted thru a Firewall to establish an IPSEC VPN tunnel to an endpoint device behind the Firewall?*

   UDP500 Standard IPSEC Tunnel or TCP 1000 if using TCP.

2. *What is IPSEC?*

   IPSEC is short for IPSecurity. According to the HyperDictionary definition, IPSec is "a protocol that provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating devices."

3. *What is IKE?*

   Internet Key Exchange refers to the key management process for IPSec VPNs.

4. *Are High Availability Firewalls a requirement for a VPN connection?*

   High availability firewalls are not a requirement for a VPN connection and actually complicate the design of the connection. If access is critical, high-availability firewalls should be used. The decision to use high-availability firewalls should be commensurate with the risks associated with a firewall outage.

5. *Are Multi-homed ISPs a requirement?*

   No, Multi-homed ISPs are used to build a high-availability solution for business continuity, but are not required.

6. *Can a virus or worm spread to my network across a VPN connection?*

   Yes, a virus may be introduced via a VPN connection just as it may from other connections. Split-tunneling which allows the remote user to be connected to other networks simultaneously increases the risks of virus introduction. Anti-virus software should be current and enabled to reduce the risks of virus infection.

7. *What level of encryption is required?*

   Technically, there is no required level of encryption for VPN. A VPN is an encrypted solution to ensure that data is transmitted in a secure manner. As long as there are no territory restrictions, Triple DES or AES (Advanced Encryption Service) should be used.

8. *How are users authenticated over a VPN connection?*

   VPNs are not directly associated with an authentication scheme. Authentication actually occurs on the terminating device. Two-factor authentication should be used for remote users to provide a higher degree of certainty the person connecting to the network is who they say they are.

9. *How do we monitor network activity over a VPN connection?*

   It is impossible to monitor the data in a VPN because it's encrypted. Monitoring on the VPN only provides information that something is being transmitted. Monitoring of user connections may be performed on the terminating device.

10. *Do VPN connections have higher bandwidth requirements?*

    No. Higher bandwidths do increase the performance of the VPN. The bandwidth requirements are really dependent upon the application. VPNs may be used with dial-up solutions.

11. Will all applications work over a VPN connection?

Most applications will work over a VPN connection. Multi-cast IP is required to support applications such as video.

12. Is a VPN required over a private point-to-point connection?

No. Private point-to-point connections are considered to be secure transports. A VPN may be used over a point-to-point connection if there is a requirement to do so. For example, it may be appropriate to use a VPN to ensure security when transferring highly sensitive data.

13. Can I establish a CISco Pix Firewall IPSEC VPN tunnel to a Checkpoint Firewall?

Yes.

14. Can I terminate a VPN connection on a router or switch?

A VPN connection may terminate on a router. It may not terminate on a switch.

15. Are there special requirements for multicast or multi-protocol support over a VPN?

IPSec only supports tunneling of unicast-IP traffic. Multicast-IP is required to run a routing protocol across the VPN and to support applications such as video. GRE can be used in conjunction with IPSec to support multicast, multi-protocols, and routing protocols.

16. Where can I find your Policies?

The Host Company will need to publish where Policies and Procedures can be accessed.

15. Do I need any special software? If yes, how do I get a copy?

Host Company will need to publish how to download copies of software and any licensing agreements.

16. How do I get technical support?

Host Company will need to publish telephone numbers and/or website addresses to receive technical support.

17. Are there any special Disconnect Procedures I should follow?

Host Company will need to publish where Policies and Procedures can be accessed.

There's more where this came from.

The American Petroleum Institute provides additional resources and programs to the oil and natural gas industry which are based on API® Standards. For more information, contact:

• API Monogram® Licensing Program	Phone:	202-962-4791
	Fax:	202-682-8070
• American Petroleum Institute Quality Registrar (APIQR®)	Phone:	202-962-4791
	Fax:	202-682-8070
• API Spec Q1® Registration	Phone:	202-962-4791
	Fax:	202-682-8070
• API Perforator Design Registration	Phone:	202-962-4791
	Fax:	202-682-8070
• API ISO/TS 29001 Registration	Phone:	202-962-4791
	Fax:	202-682-8070
• API Training Provider Certification Program	Phone:	202-682-8490
	Fax:	202-682-8070
• Individual Certification Programs	Phone:	202-682-8064
	Fax:	202-682-8348
• Engine Oil Licensing and Certification System (EOLCS)	Phone:	202-682-8516
	Fax:	202-962-4739
• API PetroTEAM™ (Training, Education and Meetings)	Phone:	202-682-8195
	Fax:	202-682-8222

Check out the API Publications, Programs, and Services Catalog online at www.api.org.

API
American Petroleum Institute

Helping You Get
The Job Done Right.®

API

Effective January 1, 2007.
API Members receive a 30% discount where applicable.
The member discount does not apply to purchases made for the purpose of resale or for incorporation into commercial products, training courses, workshops, or other commercial enterprises.

2007 Publications Order Form

Available through IHS:
Phone Orders: **1-800-854-7179** (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: **303-397-2740**
Online Orders: **global.ihs.com**

Date: _____ ❑ **API Member** (Check if Yes)

Invoice To (❑ Check here if same as "Ship To")

Name:
Title:
Company:
Department:
Address:
City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
E-Mail:

Ship To (UPS will not deliver to a P.O. Box)

Name:
Title:
Company:
Department:
Address:
City: State/Province:
Zip/Postal Code: Country:
Telephone:
Fax:
E-Mail:

Quantity	Product Number	Title	SO★	Unit Price	Total
	OS0001	Security Guidance for the Petroleum Industry		$170.00	
	OSVA02	Security Vulnerability Assessment Methodology for Petroleum and PetroChemical Industries		$170.00	
	D11641	API Standard 1164, SCADA Security		$113.00	

❑ **Payment Enclosed** ❑ **P.O. No.** (Enclose Copy) _____

❑ **Charge My IHS Account No.** _____

❑ **VISA** ❑ **MasterCard** ❑ **American Express** ❑ **Diners Club** ❑ **Discover**

Credit Card No.:

Print Name (As It Appears on Card):

Expiration Date:

Signature:

Subtotal	
Applicable Sales Tax *(see below)*	
Rush Shipping Fee *(see below)*	
Shipping and Handling *(see below)*	
Total *(in U.S. Dollars)*	

★ ***To be placed on Standing Order for future editions of this publication, place a check mark in the SO column and sign here:***

Pricing and availability subject to change without notice.

Mail Orders – Payment by check or money order in U.S. dollars is required except for established accounts. State and local taxes, $10 processing fee, and 5% shipping must be added. Send mail orders to: **API Publications, IHS, 15 Inverness Way East, c/o Retail Sales, Englewood, CO 80112-5776, USA.**
Purchase Orders – Purchase orders are accepted from established accounts. Invoice will include actual freight cost, a $10 processing fee, plus state and local taxes.
Telephone Orders – If ordering by telephone, a $10 processing fee and actual freight costs will be added to the order.
Sales Tax – All U.S. purchases must include applicable state and local sales tax. Customers claiming tax-exempt status must provide IHS with a copy of their exemption certificate.
Shipping (U.S. Orders) – Orders shipped within the U.S. are sent via traceable means. Most orders are shipped the same day. Subscription updates are sent by First-Class Mail. Other options, including next-day service, air service, and fax transmission are available at additional cost. Call 1-800-854-7179 for more information.
Shipping (International Orders) – Standard international shipping is by air express courier service. Subscription updates are sent by World Mail. Normal delivery is 3-4 days from shipping date.
Rush Shipping Fee – Next Day Delivery orders charge is $20 in addition to the carrier charges. Next Day Delivery orders must be placed by 2:00 p.m. MST to ensure overnight delivery.
Returns – All returns must be pre-approved by calling the IHS Customer Service Department at 1-800-624-3974 for information and assistance. There may be a 15% restocking fee. Special order items, electronic documents, and age-dated materials are non-returnable.

1220 L Street, NW
Washington, DC 20005-4070
USA

202.682.8000

Additional copies are available through IHS
Phone Orders: 1-800-854-7179 (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: 303-397-2740
Online Orders: global.ihs.com

Information about API Publications, Programs and Services
is available on the web at **www.api.org**

Product No. TSTP01