<Your Company Name>
THIRD PARTY CONNECTION AGREEMENT

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

This Third Party Network Connection Agreement (the "Agreement") by and between <Your Company Name>, a <Your Company's State> corporation, with principal offices at <Your Address>, <Your Company's State>, ("<Your Company>") and _____ , a _____ corporation, with principal offices at _____ ("Company"), is entered into as of the date last written below ("the Effective Date").

This Agreement consists of this signature page and the following attachments that are incorporated in this Agreement by this reference:

1. Attachment 1: Third Party Network Connection Agreement Terms and Conditions
2. Attachment 2 Network Connection Policy
3. Attachment 3: Third Party Connection Request - Information Requirements Document
4. Attachment 4: <Your Company> Non-Disclosure Agreement
5. Attachment 5: <Your Company> Equipment Loan Agreement

This Agreement is the complete agreement between the parties hereto concerning the subject matter of this Agreement and replaces any prior oral or written communications between the parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by <Your Company's State> law without regard to choice of law provisions.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed. Each party warrants and represents that its respective signatories whose signatures appear below have been and are on the date of signature duly authorized to execute this Agreement.

_____ ("Company")	<Your Company Name> ("<Your Company>")
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Name	Name
_____	_____
Date	Date

Attachment 1
THIRD PARTY CONNECTION AGREEMENT
TERMS AND CONDITIONS

Object: To ensure that a secure method of connectivity is provided between <Your Company> and Company and to provide guidelines for the use of network and computing resources associated with the Network Connection as defined below.

Definition: "Network Connection" means one of the <Your Company> connectivity options listed in Section B of the Network Connection Policy.

1. Right to Use Network Connection. Company may only use the Network Connection for business purposes as outlined by the **Third Party Connection Request - Information Requirements Document**.

2. <Your Company>-Owned Equipment.

   2.1 <Your Company> may, in <Your Company> sole discretion, loan to Company certain equipment and/or software for use on Company premises (the <Your Company>-Owned Equipment) under the terms of the <Your Company> Equipment Loan Agreement set forth in Attachment 5. <Your Company>-Owned Equipment will only be configured for TCP/IP, and will be used solely by Company on Company's premises and for the purposes set forth in this Agreement.

   2.2 Company may modify the configuration of the <Your Company>-Owned Equipment only after notification and approval in writing by authorized <Your Company> personnel.

   2.3 Company will not change or delete any passwords set on <Your Company>-Owned Equipment without prior approval by authorized <Your Company> personnel. Promptly upon any such change, Company shall provide <Your Company> with such changed password.

3. Network Security.

   3.1 Company will allow only Company employees approved in advance by <Your Company> ("Authorized Company Employees") to access the Network Connection or any <Your Company>-Owned Equipment. Company shall be solely responsible for ensuring that Authorized Company Employees are not security risks, and upon <Your Company>'s request, Company will provide <Your Company> with any information reasonably necessary for <Your Company> to evaluate security issues

relating to any Authorized Company Employee. Access to the Network Connection or any <Your Company>-Owned Equipment

3.2 Company will promptly notify <Your Company> whenever any Authorized Company Employee leaves Company's employ or no longer requires access to the Network Connection or <Your Company>-Owned Equipment.

3.3 Each party will be solely responsible for the selection, implementation, and maintenance of security procedures and policies that are sufficient to ensure that (a) such party's use of the Network Connection (and Company's use of <Your Company>-Owned Equipment) is secure and is used only for authorized purposes, and (b) such party's business records and data are protected against improper access, use, loss alteration or destruction.

4. Notifications. Company shall notify <Your Company> in writing promptly upon a change in the user base for the work performed over the Network Connection or whenever in Company's opinion a change in the connection and/or functional requirements of the Network Connection is necessary.

5. Payment of Costs. Each party will be responsible for all costs incurred by that party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

6. DISCLAIMER OF WARRANTIES. NEITHER PARTY MAKES ANY WARRANTIES, EXPRESSED OR IMPLIED, CONCERNING ANY SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY. EXCEPT WITH RESPECT TO A PARTY'S CONFIDENTIALITY OBLIGATIONS UNDER THIS AGREEMENT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, BUSINESS OR PROFITS) ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM ANY DELAY, OMISSION OR ERROR IN THE ELECTRONIC TRANSMISSION OR RECEIPT OF DATA PURSUANT TO THIS AGREEMENT, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, AND WHETHER OR NOT A PARTY

HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

8. Confidentiality. The parties acknowledge that by reason of their relationship to each other hereunder, each will have access to certain information and materials concerning the others technology and products that is confidential and of substantial value to that party, which value would be impaired if such information were disclosed to third parties ("Confidential Information"). Should such Confidential Information be orally or visually disclosed, the disclosing party shall summarize the information in writing as confidential within thirty (30) days of disclosure. Each party agrees that it will not use in any way for its own account, except as provided herein, nor disclose to any third party, any such Confidential Information revealed to it by the other party. Each party will take every reasonable precaution to protect the confidentiality of such Confidential Information. Upon request by the receiving party, the disclosing party shall advise whether or not it considers any particular information or materials to be Confidential Information. The receiving party acknowledges that unauthorized use or disclosure thereof could cause the disclosing party irreparable harm that could not be compensated by monetary damages. Accordingly each party agrees that the other will be entitled to seek injunctive and preliminary relief to remedy any actual or threatened unauthorized use or disclosure of such other party's Confidential Information. The receiving party's obligation of confidentiality shall not apply to information that: (a) is already known to the receiving party or is publicly available at the time of disclosure; (b) is disclosed to the receiving party by a third party who is not in breach of an obligation of confidentiality to the party to this agreement which is claiming a proprietary right in such information; or (c) becomes publicly available after disclosure through no fault of the receiving party.

9. Term, Termination and Survival. This Agreement will remain in effect until terminated by either party. Either party may terminate this agreement for convenience by providing not less than thirty (30) days prior written notice, which notice will specify the effective date of termination. Either party may also terminate this Agreement immediately upon the other party's breach of this Agreement. Sections 5, 6, 7, 8, 10.1 and 10.2 shall survive any termination of this Agreement.

10. MISCELLANEOUS.

10.1 Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.

10.2 Waiver. The failure of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

10.3 Assignment. Neither party may assign this Agreement, in whole or in part, without the other party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the parties' respective successors and permitted assigns.

10.4 Force Majeure. Neither party will be liable for any failure to perform its obligations in connection with any Transaction or any Document if such failure results from any act of God or other cause beyond such party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents such party from transmitting or receiving any Documents.

Attachment2
NETWORK CONNECTION POLICY

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

Scope: External company data network connections to <Your Company> can create potential security exposures if not administered and managed correctly and consistently. These exposures may include non-approved methods of connection to the <Your Company> network, the inability to shut down access in the event of a security breach, and exposure to hacking attempts. Therefore, all external company data network connections will be via the Global Partners Network. This policy applies to all new Third Party Network Connection requests and any existing Third Party Network Connections. When existing Third Party Network Connections do not meet all of the guidelines and requirements outlined in this document, they will be re-engineered as needed

Definitions: A "Network Connection" is defined as one of the connectivity options listed in Section B. below. "Third Parties" is defined as <Your Company> Partners, Vendors, Suppliers and the like.

A. Third-Party Connection Requests and Approvals

All requests for Third Party connections must be made using the appropriate method based on the support organization. [Add text about the specific support methods]

The required information is outlined in the **Third Party Connection Request - Information Requirements Document** (See Attachment 3 of this document). All information requested on this form must be completed prior to approval and sign off. It is Company's responsibility to ensure that Company has provided all of the necessary information and that such information is correct.

All Third Party connection requests must have a <Your Company> VP level signature for approval. In some cases approval may be given at a lower level with pre-authorization from the appropriate <Your Company> VP. Also, all Third Parties requesting a Network Connection must complete and sign a <Your Company> Non-Disclosure Agreement.

As a part of the request and approval process, the technical and administrative contact within Company's organization or someone at a higher level within Company will be required to read and sign the "Third Party Connection Agreement " and any additional documents, such as the <Your Company> Non-Disclosure Agreement.

B. Connectivity Options

The following five connectivity options are the standard methods of providing a Third Party Network Connection. Anything that deviates from these standard methods must have a waiver sign-off at the <Your Company> VP level.

1) Leased line (e.g. T1) - Leased lines for Third Parties will be terminated on the Partners network.

2) ISDN/FR - Dial leased lines will terminate on a Third Party only router located on the ECS or IT Partners network. Authentication for these connections must be as stated in Section E. below.

3) Encrypted Tunnel - Encrypted tunnels should[must?] be terminated on the Partners Network whenever possible. In certain circumstances, it may be required to terminate an encrypted tunnel on the dirty subnet, in which case the normal <Your Company> perimeter security measures will control access to Internal devices.

4) Telnet access from Internet - Telnet access from the Internet will be provided by first telneting to the Third Party gateway machine, where the connection will be authenticated per Section E. below. Once the connection is authenticated, telnet sessions to internal hosts will be limited to those services needed by using the authorization capabilities of <Your Company>Secure.

5) Remote Dial-up via PPP/SLIP - Remote dial-up via PPP/SLIP will be provided by a separate Third Party modem pool. The connection will be authenticated per Section E. below

C. Third Party (Partner) Access Points

When possible, Third Party (Partner) Access Points (PAPs should be established in locations such that the cost of the access is minimized. Each PAP should consist of at least one router with leased line with Frame Relay and/or ISDN capability.

D. 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. **Blanket access will not be provided for anyone.** The default policy position is to deny all access and then only allow those specific services that are needed and approved by <Your Company> pursuant to the established procedure.

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

The standard set of allowable services are listed below:

File Exchange via ftp – Where possible, file exchange via ftp should take place on the existing <Your Company> ftp servers (ftp-eng.<Your Company>.com for engineering-related work or ftp.<Your Company>.com for all other work). IT supported Third Party connections have additional FTP services provided by a server in on the Partners Network.

Electronic Mail Exchange – Business-related email exchange between <Your Company> and Third Parties may be conducted over the Network Connection as needed. Mail from Third Party sites to non-<Your Company> addresses will not be allowed over the Network Connection.

Telnet Access – Telnet access will be provided to specific <Your Company> hosts, as needed. Employees from Third Parties will only be given accounts on the specific <Your Company> hosts that are needed. Where possible, router ACLs and static routes will be used to limit the paths of access to other internal <Your Company> hosts and devices. NOTE: NIS accounts and Directory Services are not to be established for employees of Third Parties who have accounts on <Your Company> hosts.

Web Resource Access – Access to internal web resources will be provided on an as-needed basis. Access will be provided by mirroring the appropriate web resources to a web server that resides on the Partners Network. Access to <Your Company>'s public web resources will be accomplished via the normal Internet access for the Third Party.

Access to Source Code Repositories This access will be decided on case by case basis.

Print Services – Print services can be provided to <Your Company> IT-supported Third Party connections by via two print spoolers on the <Your Company> Partners Network. <Your Company>-owned printers, that boot off the print spoolers will be located on the <Your Company> – extended network at the Third Party sites.

SQL*Net Access – This will be decided on a case by case basis.

ERP Access – This will be decided on a case by case basis.

NT File Exchange – File exchange will be provided by NT file servers located on the <Your Company> Partners Network. Each Third Party needing NT File exchange will be provided with a separate folder that is only accessible to that Party and the necessary people at <Your Company>.

E. Authentication for Third Party Network Connections
Third Party Network Connections made via remote dial-up using PPP/SLIP or standard telnet over the Internet will be authenticated using the Partners Authentication database and Token Access System. Currently, <Generic> is the token access system in use. A separate server will be established specifically for Third Parties. Reports showing who has access via the tokens will be generated monthly and sent to the <Your Company> POCs for each Third Party for verification and review.

Telnet connection made via the Internet must be initiated to a separate which authenticates to the Partners Authentication database and Token Access System mentioned above..

ISDN/FR connections will be authenticated via the Partners <Your Company>Secure database, which is separate from the <Your Company> ISDN authentication database.

F. <Your Company> Equipment at Third Party Sites
In many cases it may be necessary to have <Your Company>-owned and maintained equipment at a Third Party site. All such equipment will be documented on the Third Party Connection Request – Information Requirements Document. Access to network devices such as routers and switches will only be provided to <Your Company> support personnel. All <Your Company>-Owned Equipment located at Third Party sites must be used only for business purposes. Any misuse of access or tampering with <Your Company>-provided hardware or software, except as authorized in writing by <Your Company>, may, in <Your Company>'s sole discretion, result in termination of the connection agreement with the Third Party. If <Your Company> equipment is loaned to a Third Party, the Third Party will be required to sign an appropriate <Your Company> Equipment Loan Agreement, if one is required

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

Security of Third Party Connections will be achieved by implementing "Access Control Lists" on the Partner Gateway routers to which the Third Party sites are connected. The ACLs will restrict access to pre-defined hosts within the internal <Your Company> network. The ACLs will be determined by the appropriate support organization. A set of default ACLs may be established as a baseline.

Enable-level access to <Your Company>-owned/maintained routers on Third Party premise will only be provided to the appropriate support organization. All other business personnel (i.e. Partner Site local technical support personnel) will have restricted

access/read-only access to the routers at their site and will not be allowed to make configuration changes.

<Your 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.

H. Audit and Review of Third Party Network Connections
All aspects of Third Party Network Connections - up to, but not including Company's firewall, will be monitored by the appropriate <Your Company> network support group. Where possible, automated tools will be used to accomplish the auditing tasks. Monthly reports should be generated on the Partners Authentication database showing the specific login entries and the appropriate <Your Company> POC. Each <Your Company> Partner POC will receive a copy of the monthly reports showing all of the accounts pertaining to his/her area. Copies of the reports will also be mailed to the department directors.

Nightly audits will be performed on all <Your Company>-owned/maintained Third Party router/network device configurations and the output will be mailed to the appropriate <Your Company> network support group. Any unauthorized changes will be investigated immediately.

All Third Party Network Connections will be reviewed on a quarterly basis and information regarding specific Third Party Network Connection will be updated as necessary. Obsolete Third Party Network Connections will be terminated.

I. <Your Company> Corporate IT Information Security Organization
<Your Company> Corporate IT Information Security has the responsibility for maintaining related policies and standards. Corporate IT Information Security will also provide advice and assistance regarding judgment calls, and will facilitate information gathering in order to make a correct decision. Global coordination of confidentiality and non-disclosure agreements with all third parties is also the responsibility of <Your Company> Corporate IT Information Security.

J. <Your Company> Enterprise Network Services
The Enterprise Network Services Partners Group is responsible for all global firewall design, configuration and engineering required for support of the Global Partners Network.

Attachment 3
THIRD PARTY CONNECTION REQUEST - INFORMATION REQUIREMENTS DOCUMENT

In accordance with the Network Connection Policy, all requests for Third Party Network Connections must be accompanied by this completed Information Requirements Document. This document should be completed by the <Your Company> person or group requesting the Network Connection.

A. Contact Information

Requester Information
- Name:
- Department Number:
- Manager's Name:
- Director's Name:
- Phone Number:
- Email Address:

Technical Contact Information
- Name:
- Department:
- Manager's Name:
- Director's Name:
- Phone Number:
- Pager Number:
- Email Address

Back-up Point of Contact:
- Name:
- Department:
- Manager's Name:
- Director's Name:
- Phone Number:
- Pager Number:
- Email Address

B. Problem Statement/Purpose of Connection
What is the desired end result? Company must include a statement about the business needs of the proposed connection.

C. Scope of Needs **(**In some cases, the scope of needs may be jointly determined by the supporting organization and the Third Party.)

What services are needed? (See Section D. of Network Connection Policy)
What are the privacy requirements (i.e. do you need encryption)?
What are the bandwidth needs?
How long is the connection needed?
Future requirements, if any.

D. Third Party Information
Third Party Name
Management contact (Name, Phone number, Email address)
Location (address) of termination point of the Network Connection (including building number, floor and room number)
Main phone number
Local Technical Support Hours (7X24, etc).
Escalation List
Host/domain names of the Third Party
Names (Email addresses, phone numbers) of all employees of the Third Party who will use this access. If not appropriate to list the names of all employees, then provide a count of the number of employees who will be using the connection.

E. What type of work will be done over the Network Connection?
What applications will be used?
What type of data transfers will be done?
How many files are involved?
What are the estimated hours of use each week? What are peek hours?

F. Are there any known issues such as special services that are required? Are there any unknown issues at this point, such as what internal <Your Company> services are needed?

G. Is a backup connection needed? (e.g., are there any critical business needs associated with this connection?)

H. What is the requested installation date? (Minimum lead-time is 60 days)

I. What is the approximate duration of the Third Party Network Connection?

J. Has a Non-Disclosure Agreement been sign with the Third Party or the appropriate employees of the Third Party?

K. Are there any exiting Network Connections at <Your Company> with this company?

L. Other useful information