Extranet Policy

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

1.0 Purpose
This document describes the policy under which third party organizations connect to <Company Name> networks for the purpose of transacting business related to <Company Name>.

2.0 Scope
Connections between third parties that require access to non-public <Company Name> resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for <Company Name> or to the Public Switched Telephone Network does NOT fall under this policy.

3.0 Policy

3.1 Pre-Requisites

3.1.1 Security Review
All new extranet connectivity will go through a security review with the Information Security department (InfoSec). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

3.1.2 Third Party Connection Agreement
All new connection requests between third parties and <Company Name> require that the third party and <Company Name> representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by the Vice President of the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into <Company Name> labs are to be kept on file with the [name of team responsible for security of labs].

3.1.3 Business Case
All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the [name of team responsible for security of labs]. Typically this function is handled as part of the *Third Party Agreement*.

3.1.4 Point Of Contact
The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the *Third Party Agreement* that pertain to it. In the event that the POC changes, the relevant extranet Organization must be informed promptly.

3.2 Establishing Connectivity

Sponsoring Organizations within <Company Name> that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage InfoSec to address security issues inherent in the project. If the proposed connection is to terminate within a lab at <Company Name>, the Sponsoring Organization must engage the [name of team responsible for security of labs]. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and InfoSec, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will <Company Name> rely upon the third party to protect <Company Name>'s network or resources.

3.3 Modifying or Changing Connectivity and Access
All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or InfoSec when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.4 Terminating Access
When access is no longer required, the Sponsoring Organization within <Company Name> must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct <Company Name> business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct <Company Name> business necessitate a modification of existing permissions, or termination of connectivity, InfoSec and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any action.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.
Sponsoring Organization	The <Company Name> organization who requested that the third party have access into <Company Name>.
Third Party	A business that is not a formal or subsidiary part of <Company Name>.

6.0 Revision History