<Company Name>

Remote Access Tools Usage Policy

Created 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 Overview

Remote desktop software, also known as **remote access tools**, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the <Company Name> network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on <Company Name> computer systems.

2.0 Purpose

This policy defines the requirements for remote access tools used at <Company Name>.

3.0 Scope

This policy applies to all remote access where either end of the communication terminates at a <Company Name> computer asset.

4.0 Policy

All remote access tools used to communicate between <Company Name> assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools

1. <Company Name> provides mechanisms to collaborate between internal users, with external partners, and from non-<Company Name> systems. The approved software list can be obtained from <link-to-approved-remote-access-software-list>. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.
2. The approved software list may change at any time, but the following requirements will be used for selecting approved products:
   a) All remote access tools or systems that allow communication to <Company Name> resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
   b) The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
   c) Remote access tools must support the <Company Name> application layer proxy rather than direct connections through the perimeter firewall(s).
   d) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the <Company Name> network encryption protocols policy.
   e) All <Company Name> antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.
3. All remote access tools must be purchased through the standard <Company Name> procurement process, and the information technology group must approve the purchase.

4.2 <Company Name> Ramifications

Failure to use secure, supported remote access tools may expose <Company Name> to computer intrusion activity and could lead to loss of intellectual property, revenue, and/or reputation. It is the responsibility of each employee to protect the interests of <Company Name> while utilizing <Company Name> assets and information.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate malicious activity involving theft or damage of intellectual property may be subject to criminal prosecution.

6.0 Definitions

Terms	Definitions
Application layer proxy:	An intermediary system that sits between a client and server and passes traffic only after validating the correctness of the application protocol and data.
Challenge-Response:	A protocol where one party presents a “challenge” and the other must present a “response” to be authenticated.
Data loss prevention:	A system to identify, monitor, and protect data in use, at rest, and in motion from accidental or intentional transmission.
LDAP:	Lightweight Directory Access Protocol -- a protocol for querying and modifying directory services (often user authentication information).
Replay Attack:	The use of a previously recorded authentication session in order to obtain unauthorized access.
Remote access tool:	Any of a number of tools that provide remote access to a computer system “as if” the remote user were actually sitting in front of the computer.
SecurID:	A two-factor authentication system consisting of something the user has (a “token”) and something he or she knows (the PIN).

7.0 Revision History

2010-05-04 Initial Revision. John Jarocki