Remote Access Tools Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

1. 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 LogMeIn, 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. Purpose

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

3. Scope

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

4. 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
<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.

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.

All remote access tools must be purchased through the standard <Company Name> procurement process, and the information technology group must approve the purchase.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance

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

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Application layer proxy

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.