Remote Access Tools Policy

June 2015

# Table of Contents

[Table of Contents](#_cugjqkm78ego)

[Overview](#_3b8y2wulq2r9)

[Purpose](#_7g8fatxxmevr)

[Scope](#_kioayvx3id7g)

[Policy](#_8yca70wbp2sa)

[Remote Access Tools](#_gqbyh7arknzt)

[Policy Compliance](#_f3r0vemj1xfs)

[Compliance Measurement](#_gan660xir2j3)

[Exceptions](#_elxlxpj9prs8)

[Non-Compliance](#_3xuloaj1og2)

[Related Standards, Policies and Processes](#_dt45h06wp6n0)

[Definitions and Terms](#_xzlgiakt8pdi)

[Revision History](#_iwv7gk9q8xr)

# 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 Infinity Works Consulting 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 Infinity Works Consulting computer systems.

# Purpose

This policy defines the requirements for remote access tools used at Infinity Works Consulting

# Scope

This policy applies to all remote access where either end of the communication terminates at a Infinity Works Consulting computer asset

# Policy

All remote access tools used to communicate between Infinity Works Consulting assets and other systems must comply with the following policy requirements.

## 4.1 Remote Access Tools

Infinity Works Consulting provides mechanisms to collaborate between internal users, with external partners, and from non-Infinity Works Consulting systems. The current approved software is LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP) only. 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 may change at any time, but the following requirements will be used for selecting approved products:

1. All remote access tools or systems that allow communication to Infinity Works Consulting 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.
2. 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.
3. Remote access tools must support an Infinity Works Consulting application layer proxy rather than direct connections through the perimeter firewall(s).
4. Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Infinity Works Consulting network encryption protocols policy.
5. All Infinity Works Consulting 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 Infinity Works Consulting procurement process, and the Senior Management Team (SMT) must approve the purchase.

# Policy Compliance

## Compliance Measurement

The Infinity Works Consulting Security Guild will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the Infinity Works Consulting Security Guild in advance.

## Non-Compliance

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

# Related Standards, Policies and Processes

None.

# 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

# Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| June 2015 | Infinity Works Consulting Security Guild | Updated and converted to new format |