Remote Access Tools Policy

ChilledWeb Limited

Policy Name:	Remote Access Tools Policy	Policy Ref:	CWRAAP
Date of Last Revision:	19 January 2026	Version No:	4.7

Contents

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 ChilledWeb network that can be used for theft of, unauthorised access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on ChilledWeb computer systems.

Purpose

This policy defines the requirements for remote access tools used at ChilledWeb.

Scope

This policy applies to all remote access where either end of the communication terminates at a ChilledWeb computer asset.

Policy

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

Remote Access Tools

ChilledWeb provides mechanisms to collaborate between internal users, with external partners, and from non-ChilledWeb systems. 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:

- All remote access tools or systems that allow communication to ChilledWeb 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.

- 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.
- Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the ChilledWeb network encryption protocols policy.
- All ChilledWeb 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 ChilledWeb procurement process.

Exceptions

Any exception to the policy must be approved by the Directors 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.