Remote Access Tools Policy

Last Update Status: *Updated June 2022*

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. While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the F1 TEAM 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 F1 TEAM computer systems.

2. Purpose

This policy defines the requirements for remote access tools used at F1 TEAM

3. Scope

This policy applies to all remote access where either end of the communication terminates at a F1 TEAM computer asset

4. Policy

All remote access tools used to communicate between F1 TEAM assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools

F1 TEAM provides mechanisms to collaborate between internal users, with external partners, and from non-F1 TEAM systems. The approved software is Windows RDP. 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:

a) All remote access tools or systems that allow communication to F1 TEAM resources from the Internet or external partner systems must support multi-factor authentication.
b) The authentication database source must be MIT Kerberos, 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 F1 TEAM 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 F1 TEAM network encryption protocols policy.
e) All F1 TEAM 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 F1 TEAM 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 Human Resources 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

- none

8 Revision History

Date of Change	Responsible	Summary of Change
June 2018	Human Resources Team	Updated and converted to new format.
June 2021	Human Resources Team	New F1 season.