Remote Access Tools Policy

1.0 Purpose

Remote access tools and remote desktop software (e.g., RDP, VNC, LogMeIn, GoToMyPC) offer significant benefits for productivity, collaboration, and IT support by enabling screen sharing and remote system control. However, insecure or unmanaged use of these tools creates substantial security risks, potentially providing unauthorized pathways into the organization's network, leading to data theft, unauthorized access, or system compromise. The purpose of this policy is to define the mandatory requirements for the selection, configuration, and use of remote access tools to ensure that all such access to organizational assets is secure, monitored, and controlled.

2.0 Scope

This policy applies to all employees, contractors, consultants, temporary staff, vendors, agents, and other personnel utilizing any remote access tool or technology where at least one endpoint of the communication session terminates on an organizational computer asset (e.g., server, desktop, laptop managed by the organization or connected to its network).

3.0 Policy Statements

3.1 Use of Approved Tools Only

* Only remote access tools explicitly approved and provided or sanctioned by the organization's designated IT authority (e.g., Precision Computer Team) are permitted for accessing organizational resources remotely or for allowing remote access *to* organizational assets.
* An official list of approved remote access tools and corresponding mandatory configuration procedures will be maintained by the designated IT authority and made available through internal resources. Using unapproved tools for organizational business is strictly prohibited.

3.2 Security Requirements for Approved Tools

The selection and approval of remote access tools will be based on adherence to the following minimum security requirements:

* **Multi-Factor Authentication (MFA):** All remote access originating from external networks (Internet, partner systems) into the organization's network *must* require MFA (e.g., using tokens, smart cards, authenticator apps) in addition to standard credentials.
* **Strong Authentication Source & Protocol:** Authentication must ideally leverage the organization's central identity stores (e.g., Active Directory, LDAP). Authentication protocols must be secure, resistant to replay attacks (e.g., using challenge-response mechanisms), and should mutually authenticate both endpoints of the session where technically feasible.
* **Proxy Compatibility:** Tools should support routing through organization-approved security

infrastructure, such as application layer proxies or VPN gateways, rather than requiring direct inbound connections through perimeter firewalls, unless explicitly approved as part of a secure architecture.
* **Strong Encryption:** All remote access communication channels must utilize strong, end-to-end encryption that meets or exceeds the standards defined in the organization's Acceptable Encryption Policy and relevant network security protocols.
* **Compatibility with Security Tools:** Remote access tools must not interfere with, disable, or circumvent mandatory organizational security controls deployed on endpoints or networks (e.g., antivirus/anti-malware, Data Loss Prevention (DLP), endpoint detection and response (EDR)).

3.3 Procurement and Configuration

* Any procurement of remote access tools must follow standard organizational procurement processes and requires explicit approval from the designated IT authority (e.g., Information Technology group).
* All approved remote access tools must be configured strictly according to the mandatory procedures provided by the designated IT authority to ensure secure operation.

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Information Security) will verify compliance with this policy through various methods, including network monitoring, review of approved software lists, configuration audits of endpoints and servers, security assessments of remote access infrastructure, internal/external audits, and analysis of access logs.

4.2 Exceptions

Any exception to this policy (e.g., use of a non-standard tool for a specific, justified business need with a partner) requires formal, documented justification, thorough risk assessment including compensating controls, and advance approval from the designated IT authority (e.g., Precision Computer Team or Information Security).

4.3 Enforcement

* Unauthorized remote access tools found on organizational assets will be removed.
* Network access for systems using unapproved or insecurely configured remote access tools may be blocked.
* Violations of this policy by personnel may result in disciplinary action, up to and including termination of employment or contract.

5.0 Definitions

* **Remote Access Tool:** Software or hardware that allows a user to connect to and control a computer or network resource from a remote location (e.g., RDP, VNC, VPN clients with remote control features, commercial tools like LogMeIn/GoToMyPC).

*   **Multi-Factor Authentication (MFA):** An authentication method requiring more than one verification factor (e.g., password + token code).
*   **Application Layer Proxy:** A server that acts as an intermediary for requests from clients seeking resources from other servers, specifically filtering traffic at the application layer.
*   **Mutual Authentication:** A process where both parties in a communication session authenticate each other's identity.

6.0 Related Policies

*   Remote Access Policy (Overall VPN/Network Access)
*   Acceptable Use Policy (AUP)
*   Password Policy
*   Acceptable Encryption Policy
*   Information Security Policy (Overall)
*   Procurement Policy
*   Third-Party Connection Policy

Revision #2
Created 28 August 2024 16:57:15 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery