Remote Access Policy

1.0 Purpose

Remote access to the organization's network is crucial for operational efficiency and productivity. However, connections originating from external networks, which may have lower security standards or potential compromises, introduce inherent risks. The purpose of this policy is to establish the rules and requirements for all remote connections to the organization's network. These measures are designed to minimize potential exposure and mitigate risks, including the loss or compromise of sensitive data, damage to critical systems, reputational harm, and potential legal or financial liabilities.

2.0 Scope

This policy applies to all employees, contractors, vendors, and agents of the organization ("Authorized Users") utilizing any computer or device (whether organization-owned or personally-owned) to connect to the organization's network from a remote location. This includes, but is not limited to, accessing email, intranet resources, or performing any work-related tasks on behalf of the organization. This policy encompasses all methods and technologies used for remote access.

3.0 Policy Statements

The following statements define the specific rules, responsibilities, and technical requirements governing remote access to the organization's network:

3.1 General Principles and Responsibilities

* **Security Equivalence:** Authorized Users must ensure their remote access connection security is maintained at a level equivalent to that expected within the organization's physical premises.
* **Authorized Use Only:** Access privileges are granted solely for conducting organizational business. Performance of illegal activities or pursuing outside business interests via the organization's network is strictly prohibited. Recreational use of the internet through the remote connection should be minimal and must comply with the organization's Acceptable Use Policy.
* **User Accountability:** Authorized Users are responsible for safeguarding their access credentials (logins, passwords, tokens) and preventing unauthorized use of their connection or access to organizational resources by non-Authorized Users (including family members). The Authorized User is accountable for all activities conducted through their access credentials.
* **Acceptable Use:** All remote access activities must adhere to the organization's Acceptable Use Policy.

3.2 Technical Requirements

*   **Secure Connections:** Remote access must be established using organization-approved secure methods, typically involving encryption technologies like Virtual Private Networks (VPNs). Connections must be authenticated using strong credentials, adhering to the organization's Password Policy.
*   **Endpoint Security:** All devices (organization-owned or personal) used for remote access must have organization-approved, up-to-date endpoint security software installed and active, including anti-virus/anti-malware protection. Authorized Users should utilize organization-provided resources or designated internal portals to obtain required security software.
*   **Network Isolation:** When connected to the organization's network via remote access using an organization-owned computer, Authorized Users must ensure the device is not simultaneously connected to other untrusted or public networks. Connections to personally controlled, secured home networks may be permissible if configured according to organizational guidelines. Split-tunneling configurations require explicit approval based on security assessments.
*   **Configuration Standards:** All devices used for remote access, including personally-owned equipment, must meet the minimum security configuration standards defined by the organization (as detailed in the relevant Hardware and Software Configuration Standards document).
*   **Third-Party Access:** Connections by third parties must comply with the requirements outlined in specific Third-Party Agreements and this policy.

3.3 Use of External Resources

The use of external resources (e.g., non-organizational systems or cloud services) to conduct organizational business via a remote connection requires prior approval from both the relevant business unit manager and the designated IT authority (e.g., Precision Computer team, Internal IT Security).

4.0 Compliance

4.1 Compliance Measurement

The designated IT authority (e.g., Precision Computer team, Internal IT Security) will verify compliance with this policy through various methods. These may include, but are not limited to, network monitoring, log reviews, audits (internal and external), security scans, and inspection of connected devices. Findings will be reported to the policy owner and relevant management.

4.2 Exceptions

Any exception to this policy requires formal, documented justification and advance approval from both the designated IT authority responsible for remote access services and potentially other relevant stakeholders (e.g., IT Security). Approved exceptions will be reviewed periodically.

4.3 Enforcement

Failure to comply with this policy by Authorized Users may result in disciplinary action, up to and including termination of employment or contract. Access privileges may be revoked immediately pending investigation of violations.

5.0 Related Policies and Standards

Authorized Users should familiarize themselves with the following related organizational documents:

* Acceptable Encryption Policy
* Acceptable Use Policy
* Password Policy
* Third Party Agreement / Policy
* Hardware and Software Configuration Standards for Remote Access

---

Revision #3
Created 28 August 2024 16:44:06 by Daniel O
Updated 16 September 2025 22:10:09 by Travis Woolery