Client System Access Control Policy

1.0 Purpose

This policy defines the mandatory requirements and procedures governing access to client information systems, networks, and data by Precision Computer personnel and systems. Unauthorized or excessive access to client environments represents a significant security risk to both the client and Precision Computer. The purpose of this policy is to ensure that all access to client systems is appropriately authorized, authenticated, logged, monitored, and restricted based on the principle of least privilege, thereby protecting the confidentiality, integrity, and availability of client assets.

2.0 Scope

This policy applies to all Precision Computer employees, contractors, consultants, temporary staff, and authorized third-party service providers who require or are granted access to any client-owned or client-managed IT infrastructure, applications, or data repositories via Precision Computer tools (e.g., RMM, remote access software) or direct login methods. It covers all forms of access, including administrative, user-level, read-only, and automated system access.

3.0 Policy Statements

3.1 Authorization

* Access to client systems must be explicitly authorized based on documented job roles and responsibilities related to specific client service delivery.
* Requests for access must be formally documented, justified by business need (specific client task or support function), and approved by both the relevant Precision Computer manager and, where contractually required, the client contact.
* Access levels must adhere strictly to the principle of least privilege – personnel shall only be granted the minimum level of access necessary to perform their authorized tasks for a specific client.
* Standing privileged access (e.g., Domain Admin) to client environments should be minimized. Privileged access should ideally be granted on a temporary, time-bound, and explicitly authorized basis using Privileged Access Management (PAM) solutions where feasible.

3.2 Authentication

*   **Unique Credentials:** All Precision Computer personnel accessing client systems must use unique, individual credentials. Use of shared accounts for client access is strictly prohibited.
*   **Password Requirements:** Passwords for accounts used to access client systems must comply with the Precision Computer Password Policy and should ideally meet or exceed client-specific password requirements if more stringent.
*   **Multi-Factor Authentication (MFA):** MFA is **mandatory** for all remote access by Precision Computer personnel into client networks or systems. MFA must also be used for accessing any Precision Computer management tool (e.g., RMM, PSA, Cloud Portals) that provides indirect access or control over client systems.
*   **Credential Management:** Credentials used for client access must be stored securely, never embedded in scripts or configuration files in clear text, and managed according to secure practices (e.g., using approved password managers or PAM solutions).

3.3 Access Methods and Tools

*   Access to client systems must only occur via Precision Computer-approved remote access tools and methods, as defined in the Remote Access Tools Policy.
*   Direct connections or use of unapproved tools are prohibited.
*   All remote access sessions must utilize secure, encrypted protocols (e.g., SSH, TLS-encrypted RDP, secure VPN).

3.4 Logging and Monitoring

*   All access attempts (successful and failed) to client systems by Precision Computer personnel or systems must be logged.
*   Logs must capture, at a minimum: timestamp, source IP address, Precision Computer user identity, client system accessed, type of access/protocol used, and session duration (where applicable).
*   Logs related to client system access must be forwarded to Precision Computer's central logging system (SIEM) and retained according to the Audit Logging Standard and potentially client-specific contractual requirements.
*   Logs should be regularly reviewed for anomalous or unauthorized access attempts.

3.5 Access Review

*   Access rights granted to Precision Computer personnel for client systems must be reviewed periodically (e.g., quarterly or aligned with client contract reviews) by designated Precision Computer managers.
*   Reviews must verify the continued need for access and ensure privileges align with the principle of least privilege based on current job roles and client assignments.
*   Client contacts may be involved in the review process as defined by contractual agreements.

3.6 Access Revocation

*   Access to client systems must be revoked immediately upon:
    *   Termination of employment or contract with Precision Computer.
    *   Change in job role eliminating the need for access.

    * Completion of the specific project or task requiring access.
    * Termination of the client service agreement (as part of the offboarding process).
* Revocation procedures must be documented and verifiable.

4.0 Responsibilities

* **All Personnel:** Responsible for adhering to this policy, using unique credentials, enabling MFA, and accessing client systems only via approved methods for authorized purposes.
* **Managers:** Responsible for approving access requests based on business need and least privilege, and for conducting periodic access reviews for their team members.
* **Technical Teams/Access Management:** Responsible for provisioning, modifying, and revoking access based on approved requests, implementing technical controls (MFA, logging), and maintaining access records.
* **[Designated Authority, e.g., Security Team]:** Responsible for overseeing policy compliance, auditing access logs, managing exceptions, and defining approved tools/methods.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through audits of access logs, review of access control lists and group memberships, assessment of MFA implementation, review of access request/approval documentation, periodic access reviews, and investigation of security incidents.
5.2 Exceptions: Exceptions require documented justification, risk assessment, potentially client approval, and explicit approval from the [Designated Authority].
5.3 Enforcement: Unauthorized access attempts, sharing of credentials, bypassing MFA, or other violations may result in disciplinary action, up to and including termination, and potential legal consequences.

6.0 Related Policies

* Remote Access Tools Policy
* Remote Access Policy
* Password Policy
* Audit Logging Standard
* Client Data Management Policy
* Acceptable Use Policy
* Incident Response Policy
* Client Onboarding and Offboarding Policy
* Privileged Access Management Policy (if separate)

7.0 Definitions

* **Client System:** Any IT infrastructure, application, network device, or data repository owned or managed by a client, which Precision Computer personnel access as part of service delivery.
* **Least Privilege:** The security principle of granting only the minimum permissions necessary.
* **Multi-Factor Authentication (MFA):** Authentication requiring more than one verification factor.

*   **Privileged Access Management (PAM):** Solutions and processes for securing, controlling, and monitoring access to critical administrative accounts and credentials.
*   **Remote Monitoring and Management (RMM):** Software platforms used by MSPs to remotely monitor and manage client endpoints and infrastructure.
*   **Role-Based Access Control (RBAC):** Managing access based on roles and responsibilities.

Revision #1
Created 1 May 2025 20:00:29 by Travis Woolery
Updated 16 September 2025 22:10:08 by Travis Woolery