Multi-Tenancy Security Policy

1.0 Purpose

Precision Computer utilizes shared infrastructure and platforms (multi-tenant environments) to efficiently deliver services to multiple clients. While offering scalability and cost-effectiveness, multi-tenancy introduces risks related to data segregation, access control, and resource allocation if not properly managed. The purpose of this policy is to define the mandatory security controls and architectural principles required to ensure the confidentiality, integrity, and availability of each client's data and services within shared environments, preventing unauthorized access or interference between tenants (clients).

2.0 Scope

This policy applies to all shared infrastructure, platforms, and applications managed by Precision Computer used to deliver services to multiple clients simultaneously. This includes, but is not limited to, shared hosting environments, virtualized platforms, cloud infrastructure managed by Precision Computer, shared network segments, multi-tenant applications (e.g., RMM, PSA, backup solutions, security tools), and shared databases. It applies to all personnel involved in the design, deployment, configuration, management, and security of these multi-tenant environments.

3.0 Policy Statements

3.1 Logical Segregation and Data Isolation

* Robust logical segregation controls **must** be implemented and maintained to ensure strict isolation between client tenants at all relevant layers (network, storage, compute, application, database).
* **Network Segregation:** Techniques such as VLANs, VRFs, firewalls with strict rule sets, security groups, or software-defined networking (SDN) must be used to prevent unauthorized network traffic between tenants.
* **Storage Segregation:** Data belonging to different clients must be logically separated using mechanisms like distinct storage volumes, access control lists (ACLs) on file systems/object storage, or database-level separation (e.g., separate schemas, databases, or row-level security). Encryption keys used for data-at-rest encryption should ideally be tenant-specific where feasible.
* **Compute Segregation:** Virtualization technologies must be configured securely to prevent VM escape or unauthorized inter-VM communication. Resource allocation (CPU, RAM, I/O) must be managed to prevent resource exhaustion caused by one tenant impacting others (noisy neighbor problem).

*   **Application/Database Segregation:** Multi-tenant applications must be designed or configured with strong tenant isolation controls. Unique tenant identifiers must be used throughout, and data access logic must rigorously enforce tenant boundaries.

3.2 Access Control

*   Access to the underlying shared infrastructure and management planes must be strictly controlled based on least privilege and role-based access control (RBAC).
*   Administrative access must require Multi-Factor Authentication (MFA) and comply with the Password Policy.
*   Client access to shared platforms (e.g., management portals) must be strictly limited to their own tenant data and configurations.
*   Access controls must prevent personnel assigned to one client from accessing another client's data or environment unless explicitly authorized for a specific, documented purpose (e.g., shared support function with appropriate controls).
*   All administrative access and significant configuration changes to the multi-tenant environment must be logged and monitored according to the Audit Logging Standard.

3.3 Authentication

*   Authentication mechanisms must securely identify and separate users and processes belonging to different tenants.
*   Where federated identity or single sign-on (SSO) is used, configurations must ensure that authentication tokens or assertions cannot be misused to gain cross-tenant access.

3.4 Resource Management

*   Resource allocation and monitoring must be implemented to ensure fair usage and prevent resource contention or denial-of-service conditions caused by one tenant affecting others.
*   Quota management and resource throttling may be employed.

3.5 Change Management

*   Changes to the shared infrastructure or platforms must follow the Precision Computer internal Change Management Policy.
*   Impact assessments must explicitly consider the potential effect on all tenants hosted on the platform.
*   Communication regarding maintenance or changes affecting the shared platform must be provided to all affected clients according to SLA and communication protocols.

3.6 Security Monitoring and Logging

*   The multi-tenant environment must be monitored for security events, performance issues, and availability.
*   Logging must be configured to capture tenant-specific activities where possible while ensuring logs themselves maintain tenant separation if accessed by clients.
*   Logs from the shared infrastructure must be centrally collected and analyzed according to the

Audit Logging Standard.

3.7 Vulnerability Management

* The shared infrastructure and platforms must be included in the scope of Precision Computer's Vulnerability Management program.
* Regular vulnerability scanning and timely patching according to the Patch Management Policy are required.

3.8 Penetration Testing

* Periodic penetration testing specifically targeting the multi-tenant controls and segregation mechanisms should be conducted.

4.0 Responsibilities

* **Architecture/Engineering Teams:** Responsible for designing, building, and configuring multi-tenant environments according to the security principles in this policy.
* **Operations/Infrastructure Teams:** Responsible for the day-to-day management, monitoring, patching, and maintenance of the shared infrastructure.
* **Information Security Team:** Responsible for defining security requirements, performing risk assessments, auditing controls, and overseeing vulnerability management and penetration testing of shared environments.
* **Service Delivery Teams:** Responsible for utilizing shared platforms according to defined procedures and managing client instances within them.

5.0 Compliance

5.1 Compliance Measurement: Compliance will be verified through technical audits of segregation controls, review of configurations (network, virtualization, application), vulnerability scans, penetration test results, access control reviews, log analysis, and review of relevant documentation.
5.2 Exceptions: Exceptions to this policy require rigorous technical justification, detailed risk assessment, documentation of compensating controls, and approval from senior management and the Information Security Team.
5.3 Enforcement: Failure to implement or maintain adequate security controls in multi-tenant environments can lead to significant security incidents and client data breaches. Non-compliance may result in disciplinary action and require immediate remediation efforts.

6.0 Related Policies

* Client Data Management Policy
* Client System Access Control Policy
* Network Security Policy / Firewall Policy
* Server Security Policy
* Virtualization Security Policy (if separate)
* Acceptable Encryption Policy

*   Audit Logging Standard
*   Vulnerability Management Policy
*   Change Management Policy
*   Incident Response Policy

7.0 Definitions

*   **Multi-Tenancy:** An architecture where a single instance of software and its supporting infrastructure serves multiple customers (tenants).
*   **Tenant:** A group of users (typically representing a single client organization) who share common access within a multi-tenant system but are logically isolated from other groups.
*   **Logical Segregation:** The separation of data or network traffic based on software configurations, policies, or protocols, rather than physical separation.
*   **VM Escape:** An exploit where malicious code running within a virtual machine breaks out to access the underlying hypervisor or other virtual machines.

Revision #1
Created 1 May 2025 20:01:48 by Travis Woolery
Updated 16 September 2025 22:10:09 by Travis Woolery