Change Management Policy

1.0 Purpose

This policy establishes the standard process for managing all changes to client IT environments and services managed by Precision Computer. Unauthorized or poorly managed changes can lead to service disruptions, security vulnerabilities, and client dissatisfaction. The purpose of this policy is to ensure that all changes are requested, assessed, approved, implemented, and reviewed in a controlled manner to minimize risk, avoid negative impacts on service quality and security, and maintain clear communication with clients.

2.0 Scope

This policy applies to all changes made by Precision Computer personnel or systems to client-owned or client-managed IT infrastructure, applications, configurations, or services under a management agreement. This includes, but is not limited to, hardware modifications, software installations/upgrades, operating system patching, configuration changes (network, server, application), security control adjustments, and implementation of new services or features. It covers all personnel involved in requesting, planning, approving, implementing, and reviewing changes to client environments.

3.0 Policy Statements

3.1 Change Management Principles

* All changes to client environments must follow this documented Change Management process.
* Changes must be assessed for potential impact on service availability, security, performance, and compliance.
* Changes must be appropriately authorized before implementation.
* Changes must be scheduled and communicated effectively to minimize disruption to client operations.
* All changes must be logged, tracked, and reviewed.

3.2 Change Types

Changes are categorized based on risk, impact, and urgency:

* **Standard Changes:** Low-risk, pre-authorized changes that are common, follow a documented procedure, and have minimal impact (e.g., password reset for a client user, approved software installation via RMM). Standard changes follow an expedited approval workflow defined by the Change Manager/Authority.
* **Normal Changes:** Changes that are not Standard or Emergency. They require formal risk assessment, planning, and approval through the full Change Advisory Board (CAB) process or

delegated authority based on impact.
*   **Emergency Changes:** Changes required to restore service during a critical incident or address an immediate, significant security vulnerability. These changes require expedited approval but must be fully documented, reviewed, and potentially validated retrospectively.

3.3 Change Management Process

All Normal and Emergency changes must follow these steps (Standard changes follow a defined, expedited subset):

1. **Request for Change (RFC) Submission:** Changes must be formally requested via the [MSP Name] ITSM system, detailing the change description, justification/business need, affected client(s) and Configuration Items (CIs), proposed implementation plan, risk/impact assessment, backout plan, and requested schedule.
2. **Review and Assessment:** The RFC is reviewed by the Change Manager or designated authority. A technical and business impact assessment is performed, evaluating risks, resource requirements, potential conflicts, and alignment with client configurations and agreements.
3. **Approval:**
    *   Approval is required based on the change type, risk, and impact. This may involve the requester's manager, technical subject matter experts, the Change Manager, the Change Advisory Board (CAB), and **crucially, client approval** as stipulated in the service agreement or based on the change's potential impact.
    *   The CAB (composed of representatives from technical teams, service delivery, security, and potentially account management) reviews and approves/rejects Normal changes with significant potential impact.
    *   Emergency changes require approval from authorized emergency approvers (e.g., senior management, designated on-call manager) but must still be logged.
4. **Scheduling:** Approved changes are scheduled in coordination with the client (considering business hours, maintenance windows defined in SLAs) and added to the change calendar to avoid conflicts.
5. **Implementation:** The change is implemented according to the approved plan by authorized technical personnel.
6. **Testing and Validation:** Post-implementation testing is performed to verify the change was successful and did not negatively impact related services. Client validation may be required.
7. **Closure and Review:** The RFC is updated with implementation details, test results, and closure status. Failed or problematic changes trigger backout procedures or incident management. The CAB may review implemented changes, especially Emergency changes or those with issues.

3.4 Roles and Responsibilities

*   **Change Requester:** Any authorized individual initiating a change request.
*   **Change Implementer:** Authorized technical personnel responsible for carrying out the change.
*   **Change Approver(s):** Manager(s), CAB members, Client contacts (as required), or designated authorities responsible for authorizing changes.
*   **Change Manager:** Oversees the change management process, facilitates CAB meetings,

manages the change schedule, and ensures policy adherence.
* **Change Advisory Board (CAB):** A group responsible for assessing, prioritizing, and authorizing significant Normal changes.
* **Client Contact:** Designated client representative(s) involved in approving or being notified of changes as per the service agreement.

3.5 Client Communication and Approval

* Communication with the client regarding planned changes (especially Normal and Emergency changes) is mandatory.
* Notification methods, timelines, and required approval levels will be governed by the client's Service Level Agreement (SLA) and the nature/impact of the change.
* Precision Computer must obtain explicit client approval for changes where contractually required or where the change significantly impacts client operations, cost, or risk posture.
* A forward schedule of change, including approved client maintenance windows, must be maintained and communicated appropriately.

4.0 Compliance

4.1 Compliance Measurement: Compliance will be measured through audits of RFC records in the ITSM system, review of CAB meeting minutes and approvals, analysis of change success rates, tracking of unauthorized changes identified during incident investigation, and client feedback.
4.2 Exceptions: Deviations from the standard process (e.g., for Emergency Changes) must be documented within the RFC and reviewed retrospectively by the Change Manager or CAB. Other exceptions require explicit approval from the Change Manager or designated senior management.
4.3 Enforcement: Implementing unauthorized changes or repeatedly failing to follow the change management process may result in disciplinary action, up to and including termination. Unauthorized changes causing client outages or security incidents will be treated as serious violations.

5.0 Related Policies

* Incident Management Policy (Client Focus)
* Service Level Agreement (SLA) Framework / Specific Client SLAs
* Client Communication Protocols
* Configuration Management Policy / CMDB Procedures
* Risk Management Policy
* Security Patch Management Policy
* Audit Logging Standard
* Problem Management Policy

6.0 Definitions

* **Change:** The addition, modification, or removal of anything that could have an effect on IT services delivered to a client.
* **Request for Change (RFC):** A formal proposal for a change to be made, including details of the proposed change.

*   **Configuration Item (CI):** Any component or asset that needs to be managed in order to deliver an IT service (e.g., server, router, application, documentation).
*   **Change Advisory Board (CAB):** A group of people that supports the assessment, prioritization, authorization, and scheduling of changes.
*   **IT Service Management (ITSM):** The entirety of activities performed by an organization to design, plan, deliver, operate and control IT services offered to customers.
*   **Backout Plan:** A documented plan detailing the steps required to restore a system or service to its original state if a change fails or causes unacceptable issues.

Revision #2
Created 1 May 2025 19:55:47 by Travis Woolery
Updated 16 September 2025 22:15:45 by Travis Woolery