Incident Management Policy

1.0 Purpose

This policy defines the standard process for managing operational incidents affecting client services delivered by Precision Computer. The primary goals of this policy are to ensure the timely detection, logging, categorization, resolution, and communication of incidents to restore normal service operation as quickly as possible, minimize adverse impact on client business operations, and maintain client satisfaction in accordance with Service Level Agreements (SLAs).

2.0 Scope

This policy applies to all unplanned interruptions or reductions in the quality of IT services delivered to clients by Precision Computer (referred to as "Incidents"). It covers all personnel involved in the detection, reporting, diagnosis, resolution, and communication of incidents affecting client services, including Service Desk, technical support tiers, network operations, security operations, account management, and relevant management.

This policy is distinct from the Data Breach Response Policy, which covers security incidents involving unauthorized access or data compromise, although an operational incident may escalate into a security incident.

3.0 Policy Statements

3.1 Incident Lifecycle Management

All incidents affecting client services must be managed through a defined lifecycle:

*   **Identification:** Incidents may be identified through automated monitoring systems, client reports (via phone, email, portal), or internal staff detection.
*   **Logging:** All identified incidents must be logged promptly and accurately in the Precision Computer IT Service Management (ITSM) system. The log must include relevant details such as client name, affected service(s), reported symptoms, date/time reported, source of report, and initial impact assessment.
*   **Categorization & Prioritization:** Incidents must be categorized (e.g., hardware failure, software bug, network outage, performance degradation) and prioritized based on their business impact and urgency, aligned with predefined Severity Levels (see section 3.3).
*   **Investigation & Diagnosis:** Appropriate technical personnel will investigate the incident to diagnose the root cause.
*   **Resolution & Recovery:** Actions will be taken to resolve the incident and restore normal service operation. This may involve implementing a workaround initially, followed by a permanent fix. All resolution steps must be documented in the incident log.
*   **Closure:** Once service is restored and confirmed (ideally with client validation), the incident

record will be formally closed in the ITSM system, including documentation of the final resolution.

3.2 Roles and Responsibilities

*   **Service Desk (Tier 1):** Initial point of contact for incident reporting, logging, basic troubleshooting, categorization, prioritization, resolution of simple incidents, and escalation to higher tiers.
*   **Technical Support Tiers (Tier 2/3):** Responsible for in-depth investigation, diagnosis, and resolution of escalated incidents requiring specialized knowledge.
*   **Incident Manager (or designated role):** Oversees the management of major or high-severity incidents, coordinates resources, ensures timely resolution, manages escalations, and oversees communication.
*   **Account Manager:** Acts as a liaison with the client, particularly for major incidents, ensuring client communication needs are met according to SLAs.
*   **All Personnel:** Responsible for identifying and reporting potential incidents promptly.

3.3 Severity Levels and Service Level Agreements (SLAs)

Incidents will be assigned a severity level based on impact and urgency, typically aligned with client SLAs. Examples:

*   **Severity 1 (Critical):** Complete loss of a critical business service affecting multiple users or entire site; significant business impact.
*   **Severity 2 (High):** Significant degradation or loss of a critical service affecting multiple users; major feature/functionality unavailable; significant business impact.
*   **Severity 3 (Medium):** Partial degradation of service affecting some users; minor feature/functionality unavailable; moderate business impact.
*   **Severity 4 (Low):** Minor service issue affecting a single user or minimal impact on business operations; cosmetic issue; information request.

Target response times and resolution goals are defined within individual client SLAs and are linked to these severity levels. All personnel must strive to meet or exceed SLA commitments.

3.4 Communication

*   **Internal Communication:** Clear and timely communication between support tiers, management, and account managers is essential during incident resolution.
*   **Client Communication:**
    *   Clients must be notified of Severity 1 and Severity 2 incidents affecting their services promptly, according to timelines defined in their SLA.
    *   Regular, proactive updates must be provided to affected clients throughout the lifecycle of Severity 1 and Severity 2 incidents.
    *   Communication methods (e.g., portal update, email, phone call) and frequency will be guided by the SLA and the nature of the incident.
    *   Confirmation of service restoration and incident resolution must be communicated to the client.
    *   Account Managers are responsible for ensuring client communication aligns with contractual

obligations and client expectations.

3.5 Escalation

* Incidents that cannot be resolved within the target timeframe or require additional resources must be escalated according to defined technical and managerial escalation paths.
* Escalation triggers and procedures must be documented and understood by all relevant personnel.

3.6 Major Incident Management

* Severity 1 incidents (or other incidents with significant widespread impact) will trigger a formal Major Incident Management process, typically led by an Incident Manager.
* This process involves coordinated communication (bridge calls, status updates), resource allocation, and focused efforts to restore service rapidly.

3.7 Post-Incident Review

* Major incidents (Severity 1) and recurring significant incidents require a Post-Incident Review (PIR).
* The PIR aims to identify the root cause, document lessons learned, evaluate the effectiveness of the response, and determine preventative actions to avoid recurrence.
* Findings and action items from PIRs must be tracked to completion.

4.0 Compliance

4.1 Compliance Measurement: Compliance will be measured through review of incident records in the ITSM system, analysis of SLA performance reports, client satisfaction feedback, and internal audits of the incident management process.
4.2 Exceptions: Deviations from this policy require documented justification and approval from designated management.
4.3 Enforcement: Failure to adhere to this policy may impact performance reviews, client satisfaction, and potentially lead to disciplinary action for repeated or negligent violations.

5.0 Related Policies

* Service Level Agreement (SLA) Framework / Specific Client SLAs
* Change Management Policy
* Problem Management Policy
* Data Breach Response Policy
* Client Communication Protocols
* Monitoring and Alerting Standards
* Audit Logging Standard

6.0 Definitions

* **Incident:** An unplanned interruption to an IT service or reduction in the quality of an IT service.

*   **Severity:** A measure of the business impact of an incident.
*   **Urgency:** A measure of the speed with which an incident needs to be resolved.
*   **Priority:** Determined by combining impact (Severity) and Urgency; dictates the order of handling.
*   **Workaround:** A temporary solution to reduce or eliminate the impact of an incident for which a full resolution is not yet available.
*   **Resolution:** Action taken to repair the root cause of an incident or implement a permanent fix.
*   **IT Service Management (ITSM):** The entirety of activities performed by an organization to design, plan, deliver, operate and control IT services offered to customers.
*   **Service Level Agreement (SLA):** A commitment between a service provider and a client detailing specific aspects of the service – quality, availability, responsibilities.
*   **Response Time:** The time taken from when an incident is logged until initial assessment and assignment for resolution begins.
*   **Resolution Time:** The time taken from when an incident is logged until it is resolved and normal service is restored.

Revision #2
Created 1 May 2025 19:58:31 by Travis Woolery
Updated 16 September 2025 22:16:24 by Travis Woolery