# Incident Management Plan

## NYCPS OPT Transportation Management System

### 1. Introduction

This document outlines the Incident Management process for the NYCPS Office of Pupil Transportation (OPT) Transportation Management System (TMS) provided by Sentry Management Solutions. Incident Management is a critical IT Service Management (ITSM) process focused on restoring normal service operation as quickly as possible and minimizing the adverse impact on business operations, ensuring that the best possible levels of service quality and availability are maintained.

This plan is designed to address incidents ranging from minor functional issues to major service outages, ensuring timely detection, response, resolution, and communication in alignment with the requirements and Service Level Agreements (SLAs) defined in RFP R1804 and the resulting contract.

### 2. Purpose

The primary purposes of this Incident Management Plan are to:

- Define a standardized process for managing all incidents related to the TMS solution.
- Ensure rapid detection, logging, and classification of incidents.
- Prioritize incidents based on business impact and urgency.
- Facilitate efficient investigation, diagnosis, and resolution of incidents.
- Restore normal service operation within agreed SLA targets (Ref RFP Sec 3.4, 3.25.7, 3.25.8, 3.25.21).
- Minimize the adverse impact of incidents on OPT operations, users (Drivers, Attendants, Parents, Students, School Staff, SBCs, OPT Staff), and overall service quality.
- Ensure effective communication with all relevant stakeholders during incident lifecycles.
- Provide data for Problem Management to identify and address underlying causes of recurring incidents.
- Integrate seamlessly with other service management processes like Change Management and Configuration Management.

## 3. Scope

This plan applies to any event which is not part of the standard operation of the service and which causes, or may cause, an interruption to, or a reduction in, the quality of service provided by the TMS solution. This includes, but is not limited to:

- Hardware failures or malfunctions (GPS devices, ID readers, servers, network equipment).
- Software errors, bugs, or performance degradation in any module (Driver, Parent/Student, School, Admin, Routing Engine, Backend Services).
- Integration failures with NYCPS systems (e.g., ServiceNow, Everbridge, SendGrid, Student Information Systems).
- Data integrity issues.
- Security-related events classified as incidents (to be handled in coordination with the Security Incident Response Plan outlined in `Appendix P.1 – Security Strategy.pdf`).
- Service availability issues (partial or full outages).
- Performance issues not meeting SLA targets (e.g., high latency, slow response times).
- User-reported problems or complaints regarding system functionality or service delivery received via official channels (Help Desk, In-App Feedback per Q198).

This plan works in conjunction with the Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan (Ref: `Appendix Q.1 – Business Continuity Plan And Operational Excellence.pdf`). Major disasters invoking DR procedures will follow the protocols outlined in the BCP/DR plan, although incident management processes will still apply for tracking, communication, and restoration verification.

## 4. Roles and Responsibilities

Clear roles and responsibilities are essential for effective incident management:

- **End Users (Drivers, Attendants, Parents, Students, School Staff, SBC Staff, OPT Staff):** Responsible for reporting potential incidents promptly through designated channels.
- **Sentry Management Solutions Help Desk (Tier 1 Support):** Serves as the primary point of contact for all reported incidents. Responsible for logging incidents, performing initial diagnosis and classification, resolving known errors using scripts/knowledge base, and escalating unresolved incidents to Tier 2. (Ref RFP Sec 3.3.1, 3.25.26.1)
- **Sentry Management Solutions Technical Support Teams (Tier 2 Support):** Responsible for in-depth investigation and diagnosis of incidents escalated from Tier 1. Possess specialized knowledge of specific system components (e.g., Routing Engine, Database,

Mobile Apps). Implement fixes or workarounds. Escalate complex or P1/P2 incidents to Tier 3 if necessary. (Ref RFP Sec 3.25.26.1)

- **Sentry Management Solutions Specialist/Engineering Teams (Tier 3 Support):** Provide expert-level support for complex incidents requiring deep technical knowledge, code-level analysis, or vendor engagement (for underlying COTS/platform issues). Develop permanent fixes for recurring problems identified via Problem Management. (Ref RFP Sec 3.25.26.1)
- **Sentry Management Solutions Ground Support Team (Hardware Tier 1/2):** Responsible for on-site diagnosis, repair, and replacement of GPS hardware components, coordinated via the ticketing system. (Ref RFP Sec 3.3)
- **Sentry Management Solutions Major Incident Manager (MIM):** Designated individual(s) responsible for coordinating the response to high-severity (P1/P2) incidents, ensuring effective communication, timely escalation, and adherence to resolution SLAs.
- **Sentry Management Solutions Security Team:** Responsible for leading the response to security-related incidents, working in coordination with the MIM and NYCPS security stakeholders. (Ref: `Appendix P.1 – Security Strategy.pdf`)
- **NYCPS OPT / DIIT / Relevant Staff:** Act as key stakeholders, receive incident communications, provide business impact assessment, participate in escalation reviews, approve critical actions (e.g., major changes, DR invocation), and potentially assist with Tier 3 diagnosis (per Q231).
- **School Bus Company (SBC) Administrators:** Report incidents related to their operations/drivers, coordinate hardware support access.

*Reference:* `Appendix X.1 – Team Structure and Processes.pdf`, `Appendix U.1 – Vendor and Third Party Management.pdf`, `Appendix Q.2 – Observability and Monitoring Strategy.pdf`, `Appendix U.2 – Hardware Lifecycle and Logistics Management.pdf`

---

## 5. Incident Lifecycle / Process Flow

The Incident Management process follows a defined lifecycle to ensure consistent and efficient handling of all incidents. The key stages are:

1. **Incident Detection and Logging:**
    - **Detection Methods:** Incidents can be detected through various channels:
        - Automated monitoring and alerting systems (Ref: `Appendix Q.2 – Observability and Monitoring Strategy.pdf`).
        - User reports via Help Desk (Phone, Email, Web Portal - RFP Sec 3.3.5).

        - User reports via In-App Feedback mechanisms (Parent/Student/School/Driver modules - Q198, RFP Sec 3.6.9).
        - Direct notification from NYCPS staff or SBCs.
    - **Logging:** ALL detected or reported events suspected of being incidents MUST be logged promptly in the official ticketing system (Sentry Management Solutions, integrated with NYCPS ServiceNow per Q94/Q187).
    - **Mandatory Fields:** Minimum required information at logging includes reporter details, contact information, date/time reported, affected user(s)/component(s)/service(s), and a clear description of the issue/symptoms (Ref RFP Sec 3.5.6).
2. **Incident Classification:**
    - **Categorization:** Tier 1 Support categorizes the incident based on the affected service, component, user group, and issue type (e.g., Hardware>GPS Device, Software>Routing Engine, User>Login Failure, Data>Incorrect ETA). This aids routing and analysis (Ref RFP Sec 3.5.2).
    - **Prioritization:** Incidents are prioritized based on:
        - **Impact:** The extent of disruption to business operations and the number of affected users (e.g., single user, single bus, multiple routes, entire school, system-wide). Input from OPT may be required for accurate impact assessment.
        - **Urgency:** The speed with which resolution is required, often determined by business criticality or SLA targets.

      A standard Priority Matrix (mapping Impact vs. Urgency) will be used to assign a Priority level (e.g., P1-Critical, P2-High, P3-Medium, P4-Low). P1/P2 incidents trigger the Major Incident process (see Section 6).
3. **Initial Diagnosis & Support (Tier 1):**
    - Help Desk performs initial diagnosis, checking against known error databases, FAQs (RFP Sec 3.6.12 etc.), and resolution scripts.
    - Attempts to resolve the incident immediately if possible (e.g., password reset, known workaround).
    - Updates the incident ticket with diagnostic steps taken and findings.
    - Provides initial response and status update to the reporter within SLA targets (RFP Sec 3.4.4).
    - If unable to resolve, escalates the incident to the appropriate Tier 2 Support group based on classification.
4. **Investigation and Diagnosis (Tier 2/3):**

- Tier 2 technical teams perform in-depth investigation using diagnostic tools, logs, and monitoring data.
- Engages other teams or Tier 3 specialists/engineers as needed for complex issues.
- Identifies the root cause or contributing factors if possible during the incident lifecycle (though full RCA is part of Problem Management).
- Documents all findings and actions within the incident ticket.
- Develops a workaround or permanent resolution plan.

5. **Resolution and Recovery:**
    - Applies the identified fix or workaround (e.g., deploying a code fix, restarting a service, replacing hardware, applying configuration change).
    - Changes required for resolution follow the established Change Management process (Ref: `Appendix O.2.2 – Project and Change – Risk Management Methodology.pdf`), especially for P1/P2 incidents or production changes.
    - Verifies that the fix has resolved the issue and service has been restored.
    - Tier 1 Support confirms resolution with the user who reported the incident.
6. **Incident Closure:**
    - Once resolution is confirmed, Tier 1 Support formally closes the incident ticket.
    - Final categorization, resolution details (trouble found, cause, fix applied - RFP Sec 3.5.2), and resolution time are recorded accurately.
    - Relevant Knowledge Base articles are updated or created based on the incident resolution.
    - For P1/P2 incidents, triggers the Post-Incident Review process (see Section 7).

*Reference:* `Appendix Q.2 – Observability and Monitoring Strategy.pdf` *(Process Flow, Ticketing Details),* `Appendix X.1 – Team Structure and Processes.pdf` *(Roles),* `Appendix O.2.2 – Project and Change – Risk Management Methodology.pdf` *(Change Integration),* `Appendix M.2 – Solution Design Functional and Non Functional Requirements.pdf` *(User Feedback Channels)*

---

## 6. Major Incident Process

Major Incidents (typically classified as P1 - Critical or P2 - High based on the Priority Matrix defined in Section 5.2) require an accelerated, coordinated response to minimize significant business impact and restore service as rapidly as possible. The following process is invoked when a Major Incident is declared:

1. **Declaration:**
    - An incident is formally declared a "Major Incident" by Sentry Management Solutions Help Desk Supervisor, On-Call Lead Engineer, or designated OPT contact based on exceeding pre-defined impact/urgency thresholds (e.g., system-wide outage, critical function unavailable impacting large user group, significant data integrity risk, security breach).
2. **Notification & Mobilization:**
    - Immediate notification is sent via multiple channels (e.g., automated alerts, pages, calls) to the pre-defined Major Incident Response Team roster.
    - Key personnel assemble on a dedicated communication channel (e.g., conference bridge, dedicated Slack/Teams channel) established immediately by the Major Incident Manager (MIM).
3. **Roles & Coordination:**
    - **Major Incident Manager (MIM):** Takes overall command of the incident response. Facilitates communication, coordinates efforts between technical teams, ensures process adherence, manages escalations, and provides status updates to stakeholders. This role is covered 24/7 via an on-call rotation.
    - **Technical Lead(s):** Subject matter experts for the affected component(s) responsible for leading the technical investigation, diagnosis, and proposing/implementing solutions.
    - **Communication Lead:** (Often the MIM or designated individual) Responsible for crafting and disseminating timely, accurate status updates to internal teams, NYCPS stakeholders (OPT, DIIT), and potentially external users (via pre-approved channels/templates).
    - **Resolver Groups:** Technical teams (Tier 2/3 Support, Development, Infrastructure, Security, Database, Network) actively working on diagnosis and resolution under the coordination of the MIM and Technical Lead(s).
    - **NYCPS Stakeholders:** Provide input on business impact, approve critical actions (e.g., service restarts, data restoration), and receive status updates.
4. **Diagnosis & Investigation:**
    - Focused effort to quickly identify the cause and impact of the incident using monitoring tools, logs, and collaborative troubleshooting on the established communication channel.
    - Prioritization focuses on service restoration first (workaround) before full root cause analysis (which follows in Problem Management).

5. **Resolution & Recovery:**
    - Implement workaround or fix to restore service. This may involve emergency changes, which follow an expedited Change Management process with appropriate approvals (Ref: `Appendix O.2.2 – Project and Change – Risk Management Methodology.pdf`).
    - Utilize BCP/DR procedures if necessary (e.g., failover, restoration from backup - Ref: `Appendix Q.1 – Business Continuity Plan And Operational Excellence.pdf`).
    - Continuously validate service restoration attempts.
6. **Communication Cadence:**
    - Regular status updates provided by the Communication Lead to stakeholders at agreed intervals (e.g., every 15/30/60 minutes depending on severity and phase).
    - Updates include current status, business impact, actions being taken, expected resolution time (if known), and any required user actions.
7. **Resolution Confirmation & Closure:**
    - Once service is restored and validated by technical teams and key business stakeholders, the MIM declares the Major Incident resolved.
    - Final communications are sent out.
    - The incident ticket is updated with resolution details and formally closed according to the standard process (Section 5.6).
    - The MIM initiates the Post-Incident Review (PIR) process (Section 7).

*Reference: `Appendix Q.2 – Observability and Monitoring Strategy.pdf` (Major Incident Definition, Escalation Triggers), `Appendix X.1 – Team Structure and Processes.pdf` (Roles, On-Call), `Appendix X.2 – Communications and Status Reporting Strategy.pdf` (Stakeholder Comms), `Appendix Q.1 – Business Continuity Plan And Operational Excellence.pdf` (DR Invocation), `Appendix O.2.2 – Project and Change – Risk Management Methodology.pdf` (Emergency Change Process)*

---

## 7. Post-Incident Review (PIR)

Following the resolution of every Major Incident (P1/P2) and potentially for recurring or significant lower-priority incidents, a formal Post-Incident Review (PIR) is conducted to identify lessons learned and prevent recurrence.

1. **Triggering PIR:**
    - Automatically triggered upon closure of any P1 or P2 incident.

- Can be requested by the Incident Manager, Problem Manager, or NYCPS stakeholders for other significant or recurring incidents.

2. **Timing & Participants:**
    - The PIR meeting is typically scheduled within [e.g., 3-5 business days] of incident resolution to ensure details are fresh.
    - Mandatory attendees include the Major Incident Manager (MIM), key technical leads/resolvers involved, Problem Management representative, and relevant NYCPS stakeholders. Other support staff may be invited as needed.

3. **PIR Process:**
    - **Timeline Review:** Establish a factual timeline of events from detection to resolution using incident ticket data, monitoring logs, and team inputs.
    - **Impact Assessment:** Review the confirmed business impact, affected services/users, and SLA breaches.
    - **Root Cause Analysis (RCA):** Analyze the diagnostic findings to determine the underlying root cause(s) of the incident. Differentiate between triggering events and fundamental causes. This feeds into the Problem Management process.
    - **What Went Well:** Identify aspects of the incident response that were effective (e.g., quick detection, effective communication, successful workaround).
    - **What Could Be Improved:** Identify areas where the response could have been faster or more effective (e.g., monitoring gaps, diagnostic challenges, communication delays, process shortcomings).
    - **Action Items:** Define specific, measurable, achievable, relevant, and time-bound (SMART) corrective and preventative action items assigned to owners. These aim to address root causes and improve future responses (Ref RFP Sec 3.4.5 requires corrective actions). Examples include bug fixes, infrastructure changes, monitoring enhancements, documentation updates, process adjustments, or training needs.

4. **PIR Report & Follow-up (RFP Sec 3.4.5):**
    - A formal PIR report is generated, summarizing the incident, timeline, impact, root cause(s), lessons learned, and agreed-upon action items with owners and due dates.
    - This report is distributed to attendees and key stakeholders, including NYCPS personnel, within the contractually agreed timeframe (e.g., 48 hours post-resolution as per RFP Sec 3.4.5, although PIR meeting may be slightly later).
    - Action items are tracked to completion through standard project or operational task management processes, often managed by Problem Management.

*Reference: `Appendix Q.2 – Observability and Monitoring Strategy.pdf` (PIR Process), `Appendix 0.2.2 – Project and Change – Risk Management Methodology.pdf` (Problem Management Integration, Action Item Tracking), `Appendix X.2 – Communications and Status Reporting Strategy.pdf` (Report Distribution)*

---

## 8. Incident Communication

Timely, accurate, and consistent communication is vital during incident management to keep stakeholders informed, manage expectations, and facilitate resolution.

1. **Purpose:**
    - To acknowledge reported incidents promptly.
    - To provide regular status updates on investigation and resolution progress, especially for Major Incidents.
    - To inform stakeholders of the business impact and expected resolution time (ETA), if known.
    - To notify users of workarounds or required actions.
    - To confirm service restoration.
    - To distribute Post-Incident Review findings and action plans.
2. **Target Audiences:** Communication strategies are tailored to different audiences:
    - **Internal Technical Teams:** Detailed technical updates via ticketing system, dedicated communication channels (e.g., Slack/Teams, conference bridges during Major Incidents).
    - **Sentry Management Solutions Management:** Summarized status reports, escalation notifications.
    - **NYCPS OPT / DIIT Stakeholders:** Business impact assessments, regular status updates (frequency based on priority), PIR reports, escalation notifications.
    - **SBC Administrators:** Notifications regarding service disruptions affecting their operations, device issues, or required actions.
    - **School Administrators:** Alerts regarding delays or service issues impacting their school (via School Module alerts and potentially email - RFP Sec 3.9.5, Q215).
    - **Parents/Caregivers:** Proactive notifications for significant delays or service disruptions affecting their child's route (via Parent Module app push notifications or potentially external platforms per RFP Sec 3.10.12). Communication must be clear and non-technical.

- **Drivers/Attendants:** Real-time operational alerts via Driver Module (e.g., route changes, hazards - RFP Sec 3.7.8).

3. **Communication Channels:**
    - **Ticketing System:** Primary channel for logging all incident details, technical updates, and resolution steps. Provides audit trail.
    - **Email:** Used for formal notifications to stakeholder groups (e.g., status summaries, PIR reports).
    - **Status Page:** [Optional but recommended] A dedicated status page providing real-time updates on major system issues accessible to relevant stakeholders.
    - **Conference Bridge / Dedicated Chat Channel:** Used for real-time coordination during Major Incidents.
    - **In-App Notifications:** For targeted alerts within Parent, Driver, School modules.
    - **NYC Messaging Platforms (Everbridge/SendGrid - Q98/Q175/Q230):** Used for distributing critical alerts or mass notifications to specific stakeholder groups as configured and agreed with NYCPS (e.g., alerts based on GIS events per RFP Sec 3.10.12).

4. **Communication Content & Frequency:**
    - Initial acknowledgement confirms receipt and provides the incident ticket number.
    - Updates (especially for Major Incidents) occur at regular, defined intervals and include: current status, impact assessment, actions underway, next steps, and ETA if available.
    - Communications are factual, clear, concise, and avoid speculation or blame.
    - Resolution notification confirms service restoration and any necessary follow-up actions for users.
    - Post-Incident Reports summarize the event, root cause, and corrective actions (RFP Sec 3.4.5).

*Reference:* `Appendix X.2 – Communications and Status Reporting Strategy.pdf` *(Core Communication Plan),* `Appendix Q.2 – Observability and Monitoring Strategy.pdf` *(Incident Comms Process),* `Appendix M.1 – System Architecture.pdf` *(Notification/Alerting Services, Integration Points),* `Appendix X.1 – Team Structure and Processes.pdf` *(Comms Roles - MIM etc.),* `Appendix Q.1 – Business Continuity Plan And Operational Excellence.pdf` *(BCP/DR Comms)*

---

## 9. Escalation Procedures

Escalation procedures ensure that incidents receive the appropriate level of attention and resources based on their severity, impact, or lack of progress towards resolution within SLA targets.

1. **Functional Escalation:**
    - **Purpose:** To engage teams with greater technical expertise when the current support tier cannot resolve the incident.
    - **Process:**
        - Tier 1 (Help Desk) escalates unresolved incidents to the appropriate Tier 2 Technical Support Team based on incident categorization.
        - Tier 2 escalates to Tier 3 (Specialists/Engineering) if they lack the necessary expertise, require code-level changes, or suspect a deeper platform issue.
        - Escalation includes transferring the incident ticket with all diagnostic information gathered so far.
2. **Hierarchical Escalation:**
    - **Purpose:** To alert management and ensure appropriate resources and priority are assigned, particularly when resolution is delayed or impact is severe.
    - **Triggers:**
        - Declaration of a Major Incident (P1/P2).
        - Incident resolution exceeding defined SLA timeframes for its priority level.
        - Significant unexpected increase in incident scope or impact.
        - Request from NYCPS stakeholders.
        - Lack of progress by the assigned resolver group.
    - **Process:**
        - Escalation follows a defined path, typically involving Support Team Leads, Service Delivery Managers, potentially Sentry Management Solutions Senior Management, and designated NYCPS points of contact.
        - For standard service issues (RFP Sec 3.3.7): Unresolved issues escalate functionally first, then hierarchically if delays persist (e.g., involving Tier 2 leads after 3 hours, Tier 3 leads after 6 hours for service-impacting issues).
        - For business-impacting issues (RFP Sec 3.3.8): Immediate escalation to Tier 3 support, followed by executive-level involvement within 6 hours if unresolved.
        - The Major Incident Manager (MIM) manages hierarchical escalations during Major Incidents.

3. **Third-Party/Vendor Escalation:**
    - If an incident's root cause is determined to lie with a third-party service or underlying platform (e.g., cloud provider, hardware manufacturer, integrated NYCPS system), established vendor support channels and escalation procedures are invoked.
    - Sentry Management Solutions manages these vendor escalations and communicates progress back through the incident ticket. (Ref: `Appendix U.1 – Vendor and Third Party Management.pdf`)

*Reference: `Appendix Q.2 – Observability and Monitoring Strategy.pdf` (Escalation Rules/Triggers), `Appendix X.1 – Team Structure and Processes.pdf` (Support Tiers, Management Roles), `Appendix U.1 – Vendor and Third Party Management.pdf` (Vendor Escalation Contacts/Processes), `Appendix Q.1 – Business Continuity Plan And Operational Excellence.pdf` (Escalation during DR)*

---

## 10. Reporting and Metrics

Regular reporting on incident management performance provides visibility into operational health, identifies trends, and drives continuous improvement.

1. **Data Source:** All metrics and reports are generated primarily from the data captured within the integrated ticketing system (Sentry Management Solutions / ServiceNow).
2. **Key Metrics Tracked:** We track and report on metrics including, but not limited to:
    - Total number of incidents logged (by priority, category, status, SBC, location, etc.).
    - Incident resolution times (Mean Time to Resolve - MTTR) vs. SLA targets.
    - Incident response times (Mean Time to Acknowledge/Respond - MTTA) vs. SLA targets (RFP Sec 3.4.4).
    - First Call Resolution (FCR) rate by Tier 1 Support.
    - Incident backlog (number of open incidents by age and priority).
    - Reopened incident rate.
    - Number of Major Incidents declared.
    - SLA achievement percentages.
    - Resolution details analysis (most common causes, fixes, affected components - RFP Sec 3.5.2, 3.5.11).
    - Ticket duration analysis (creation to closure, time spent in each status/group - RFP Sec 3.5.9).
    - Hardware repair/replacement statistics (linked from hardware lifecycle management).

3. **Reporting Frequency & Format:**
    - **Dashboards (RFP Sec 3.5.10):** Near real-time operational dashboards provide visibility into current ticket status (pending, active, completed) and key daily metrics.
    - **Periodic Reports:** Standard reports summarizing key metrics are generated and distributed to NYCPS stakeholders at agreed frequencies (e.g., weekly, monthly, quarterly). Formats include [Specify formats, e.g., PDF summaries, Excel data exports].
    - **Custom Reports:** Authorized NYCPS users can generate custom reports via the Admin Module reporting interface (Ref Sec 3.10.45.b).
    - **Post-Incident Reports (RFP Sec 3.4.5):** Generated within 48 hours of Major Incident resolution.
4. **Trend Analysis:** Reporting capabilities support trend analysis to identify recurring issues, systemic problems, areas needing process improvement, or potential training needs. This analysis feeds into the Problem Management process.

*Reference:* `Appendix Q.2 – Observability and Monitoring Strategy.pdf` *(Metrics, Dashboards, Reporting Process),* `Appendix S.3 – Data Engineering and Analytics Capabilities.pdf` *(Reporting Capabilities, Trend Analysis),* `Appendix X.2 – Communications and Status Reporting Strategy.pdf` *(Reporting Cadence/Distribution)*

---

## 11. Integration with Other Processes

Effective Incident Management does not operate in isolation. It integrates closely with other key ITSM and project management processes:

1. **Problem Management:**
    - Incident Management provides the primary input for Problem Management by identifying recurring incidents or single major incidents requiring root cause analysis (RCA).
    - Incident records contain valuable diagnostic information used during RCA.
    - Problem Management identifies underlying causes and proposes permanent solutions or known errors, which are then fed back into the Incident Management knowledge base to improve first call resolution rates.
    - PIR findings directly inform Problem Management investigations.

    *Ref:* `Appendix Q.2 – Observability and Monitoring Strategy.pdf`, `Appendix O.2.2 – Project and Change – Risk Management Methodology.pdf`
2. **Change Management:**

- Resolving incidents often requires changes to the IT infrastructure or application code.
- All changes resulting from incidents (especially non-standard or emergency changes) must follow the established Change Management process for assessment, approval, scheduling, and implementation to minimize unintended consequences.
- Emergency Changes needed for Major Incident resolution follow an expedited approval process defined within the Change Management plan.

*Ref:* `Appendix O.2.2 – Project and Change – Risk Management Methodology.pdf`, `Appendix N.2.1 – DevOps Strategic Framework.pdf`

3. **Configuration Management:**
    - Accurate Configuration Item (CI) information (e.g., details on specific servers, software versions, network devices, GPS hardware models) stored in a Configuration Management Database (CMDB) or equivalent asset system is crucial for effective incident diagnosis and impact assessment.
    - Incident records are linked to affected CIs.
    - Changes implemented to resolve incidents must update the corresponding CI records.

*Ref:* `Appendix M.1 – System Architecture.pdf`, `Appendix U.2 – Hardware Lifecycle and Logistics Management.pdf`, `Appendix Q.2 – Observability and Monitoring Strategy.pdf`

4. **Service Level Management:**
    - Incident Management performance (response times, resolution times) is measured against the defined SLAs.
    - Reporting on SLA achievement is a key output of Incident Management.
    - SLA breaches trigger escalation procedures within Incident Management.

*Ref:* `Appendix U.1 – Vendor and Third Party Management.pdf` *(SLAs),* `Appendix Q.2 – Observability and Monitoring Strategy.pdf` *(Reporting)*

5. **Knowledge Management:**
    - Resolutions, workarounds, and diagnostic procedures identified during Incident Management are captured and documented in a shared Knowledge Base.
    - Tier 1 Support utilizes the Knowledge Base to improve FCR.
    - PIR outputs contribute to updating or creating new knowledge articles.

*Ref:* `Appendix X.1 – Team Structure and Processes.pdf`, `Appendix T.1 – User Onboarding and Training Strategy.pdf` *(Documentation)*

6. **Business Continuity / Disaster Recovery:**
    - Incident Management identifies major disruptions that may require invocation of BCP/DR plans.

- During a DR event, Incident Management processes continue to track status, manage communications, and verify service restoration according to BCP/DR objectives.

*Ref:* `Appendix Q.1 – Business Continuity Plan And Operational Excellence.pdf`

---

## 12. Plan Review and Maintenance

This Incident Management Plan is a living document and will be reviewed and updated regularly to ensure its continued effectiveness and alignment with NYCPS OPT operational needs, contractual requirements, and evolving best practices.

1. **Review Frequency:** This plan will be formally reviewed at least annually, or more frequently if significant changes occur, such as:
    - Major system upgrades or architectural changes.
    - Changes to NYCPS policies or regulatory requirements.
    - Significant changes to the support structure or tooling.
    - Lessons learned from major incidents or recurring problems identified through Problem Management.
    - Updates to related plans (e.g., BCP/DR Plan, Security Plan).
2. **Review Process:**
    - The review will be coordinated by the Sentry Management Solutions Service Delivery Manager or equivalent role responsible for ITSM processes.
    - Participants will include representatives from Sentry Management Solutions support tiers, relevant technical teams, and designated NYCPS OPT stakeholders.
    - The review will assess the plan's effectiveness based on incident metrics, PIR findings, stakeholder feedback, and alignment with current operations.
3. **Update & Approval:**
    - Necessary updates identified during the review will be incorporated into the plan document.
    - Significant changes to the plan require formal approval from both Sentry Management Solutions management and designated NYCPS OPT representatives through the established governance process.
    - The updated plan will be communicated to all relevant internal and external stakeholders.
    - Version control will be maintained for the document.

*Reference:* `Appendix X.2 – Communications and Status Reporting Strategy.pdf` *(Governance Process),* `Appendix 0.2.2 – Project and Change – Risk Management Methodology.pdf` *(Change Management for Processes)*

---

## 13. Service Level Agreement (SLA)

This section defines the comprehensive Service Level Agreement (SLA) for incident management, customer service, and technical support for the NYCPS OPT Transportation Management System. These SLAs establish measurable performance metrics, response and resolution timeframes, and quality standards that Sentry Management Solutions commits to maintaining throughout the contract term.

### 13.1 Incident Response and Resolution SLAs

| Priority Level | Definition | Initial Response Time | Status Update Frequency | Resolution Time Target | Resolution Time Limit |
|---|---|---|---|---|---|
| **P1 - Critical** | System-wide outage or critical function unavailable affecting multiple schools or routes; student safety at risk; production environment inaccessible; complete failure of a major system component. | 15 minutes (24x7x365) | Every 30 minutes | 2 hours | 4 hours |
| **P2 - High** | Significant degradation of service; major function unavailable affecting multiple users; core feature not working; severe performance issue impacting multiple users; security vulnerability requiring immediate attention. | 30 minutes (24x7x365) | Every 1 hour | 4 hours | 8 hours |
| **P3 - Medium** | Limited impact on operations; non-critical function unavailable or working incorrectly; workaround exists; isolated performance | 2 hours (Business Hours) | Every 4 hours | 8 hours | 16 hours |

| | | | | | |
|---|---|---|---|---|---|
| | issue; affects limited number of users. | | | | |
| **P4 - Low** | Minimal impact; cosmetic issue; documentation error; feature request; question; single user affected; easy workaround available. | 4 hours (Business Hours) | Every 24 hours | 3 business days | 5 business days |

### 13.2 Support Availability SLAs

| Support Tier | Hours of Operation | Availability Target | Coverage |
|---|---|---|---|
| **Tier 1 Support (Help Desk)** | 24x7x365 | 99.9% (No more than 8.76 hours of downtime per year) | Phone, Email, Web Portal, In-App Support |
| **Tier 2 Support (Technical)** | 6:00 AM - 9:00 PM ET, Monday-Friday<br>6:00 AM - 4:00 PM ET, Saturday-Sunday<br>On-call for P1/P2 incidents 24x7x365 | 99.5% during operational hours | All technical components |
| **Tier 3 Support (Specialist/Engineering)** | 8:00 AM - 8:00 PM ET, Monday-Friday<br>On-call for P1/P2 incidents 24x7x365 | 99% during operational hours | Complex issues, code-level troubleshooting |
| **Hardware Support (Field Service)** | 8:00 AM - 6:00 PM ET, Monday-Friday | 98% of scheduled appointments met | On-site hardware repair/replacement |

### 13.3 System Performance SLAs

| Metric | Target | Measurement Method |
|---|---|---|

| | | |
|---|---|---|
| **System Availability** | 99.9% uptime during business hours (5:00 AM - 9:00 PM ET, M-F)<br>99.5% uptime during all other times<br>Excludes scheduled maintenance windows | Automated monitoring system with independent verification |
| **Transaction Response Time** | 95% of all web transactions complete in ≤ 2 seconds<br>99% of all web transactions complete in ≤ 5 seconds | Synthetic transaction monitoring |
| **Mobile App Response Time** | 95% of all mobile transactions complete in ≤ 3 seconds<br>99% of all mobile transactions complete in ≤ 7 seconds | Mobile app performance monitoring |
| **API Response Time** | 95% of API calls complete in ≤ 1 second<br>99% of API calls complete in ≤ 3 seconds | API gateway monitoring |
| **Batch Processing** | All daily batch processes completed within agreed window | Process completion monitoring |

### 13.4 Quality and Satisfaction SLAs

| Metric | Target | Measurement Method |
|---|---|---|
| **First Call Resolution (FCR)** | ≥ 75% of eligible incidents resolved during first contact | Ticketing system with post-call verification |
| **Ticket Reopening Rate** | ≤ 8% of closed tickets reopened within 7 days | Ticketing system analytics |
| **Customer Satisfaction (CSAT)** | ≥ 4.2/5.0 average score on post-incident surveys | Automated survey after ticket closure |
| **Help Desk Call Quality** | ≥ 95% compliance with quality standards during evaluations | Random call monitoring and evaluation |
| **SLA Compliance Rate** | ≥ 95% of incidents resolved within SLA timeframes | Monthly SLA compliance reporting |

### 13.5 Technical Support Tier Structure

The TMS support model employs a three-tiered approach to ensure efficient incident resolution while maximizing first-call resolution and minimizing escalations:

#### 13.5.1 Tier 1 Support - Help Desk

- **Responsibilities:**
  - Initial point of contact for all user-reported incidents and service requests
  - Incident logging, categorization, and prioritization
  - Basic troubleshooting and resolution of known issues using documented procedures
  - User account management (password resets, access issues)
  - Hardware break/fix coordination
  - Basic application usage questions
  - Escalation to appropriate Tier 2 team for complex issues
- **Staffing:** Dedicated help desk analysts with 24x7x365 coverage, multi-channel support capabilities, and knowledge of transportation operations
- **Target Resolution Rate:** 70-75% of all incidents resolved at Tier 1
- **Tools:** Ticketing system, knowledge base, monitoring dashboards, remote support tools, diagnostic scripts
- **Performance Metrics:** First-call resolution rate, average handle time, customer satisfaction, SLA compliance, abandon rate (< 5%)

#### 13.5.2 Tier 2 Support - Technical Support

- **Responsibilities:**
  - In-depth technical troubleshooting of complex issues
  - Specialized support for specific system components (routing engine, mobile apps, integration interfaces, database)
  - Detailed log analysis and error investigation
  - Configuration changes and adjustments
  - Implementing workarounds and temporary fixes
  - Coordination with third-party vendors when necessary
  - Knowledge base content creation and maintenance
  - Tier 1 staff coaching and knowledge transfer
- **Staffing:** Technical specialists with domain expertise in specific system components

- **Target Resolution Rate:** 20-25% of all incidents resolved at Tier 2
- **Tools:** Advanced diagnostic tools, database access, configuration management tools, testing environments
- **Performance Metrics:** Resolution time, escalation rate to Tier 3, SLA compliance, knowledge article creation

#### 13.5.3 Tier 3 Support - Specialist/Engineering

- **Responsibilities:**
  - Expert-level troubleshooting of the most complex issues
  - Root cause analysis of major incidents
  - Code-level investigation and debugging
  - Development of permanent fixes and patches
  - System architecture assessment and optimization
  - Performance tuning and capacity planning
  - Security vulnerability assessment and remediation
  - Coordination with development teams for feature enhancements
- **Staffing:** Senior engineers, developers, database administrators, and system architects
- **Target Resolution Rate:** 5-10% of all incidents escalated to Tier 3
- **Tools:** Development environments, source code access, advanced monitoring and profiling tools, testing platforms
- **Performance Metrics:** Root cause identification rate, permanent fix implementation, recurring incident reduction

### 13.6 SLA Monitoring and Reporting

- **Measurement:** All SLA metrics are continuously monitored and measured through automated systems, with reports generated weekly and monthly.
- **Compliance Tracking:** SLA compliance reports will be provided to NYCPS OPT stakeholders monthly, with detailed breakdowns by incident category, priority, and support tier.
- **Dashboards:** Real-time SLA compliance dashboards will be accessible to authorized NYCPS personnel through the Admin Portal.
- **Review Cadence:** Formal SLA performance reviews will be conducted quarterly with NYCPS stakeholders to identify trends, address concerns, and implement improvements.

- **Continuous Improvement:** SLA metrics and targets will be reviewed annually and adjusted as needed based on operational changes, technology evolution, and business needs.

### 13.7 SLA Exceptions and Limitations

The following circumstances are excluded from SLA calculations:

- Scheduled maintenance windows with proper advance notification
- Force majeure events (natural disasters, acts of war, etc.)
- Incidents caused by NYCPS infrastructure or systems outside Sentry Management Solutions's control
- Incidents resulting from unauthorized changes or modifications by NYCPS personnel or third parties
- Delays in resolution due to inability to access necessary NYCPS resources or personnel
- Performance issues due to exceeding agreed system capacity limitations

### 13.8 SLA Penalties and Remedies

Should Sentry Management Solutions fail to meet the defined SLA targets, the following remedies will apply:

- **Critical SLA Breach (P1 Incidents):** Credit of [X%] of monthly service fees for each documented instance
- **Recurring SLA Breaches:** Credits escalate for consecutive monthly failures to meet SLA targets
- **Chronic Underperformance:** Trigger for executive review, remediation plan, and potential contract penalties

Specific penalty structures and credit calculations are detailed in Appendix A of the Master Services Agreement.

---

## 14. Standard Operating Procedures (SOP)

This section defines the comprehensive Standard Operating Procedures (SOPs) for incident management, customer service, and technical support for the NYCPS OPT Transportation Management System. These SOPs establish detailed workflows, processes, and protocols that ensure consistent, efficient, and effective handling of all incidents and service requests.

### 14.1 Incident Detection and Reporting SOP

#### 14.1.1 Automated Detection Procedure

1. **Monitoring System Configuration:**
    - Configure monitoring thresholds for all critical system components in accordance with baseline performance metrics
    - Implement synthetic transaction monitoring to simulate key user workflows every 5 minutes
    - Set up real-time database query monitoring to detect performance degradation
    - Establish API endpoint availability and response time checks
    - Configure mobile app performance monitoring
2. **Alert Generation and Notification:**
    - Classify alerts by severity (Warning, Error, Critical) based on predefined thresholds
    - Route alerts to appropriate teams based on component and severity
    - Implement escalation for unacknowledged Critical alerts after 15 minutes
    - Maintain alert suppression rules to prevent notification storms
3. **Alert Verification:**
    - On-call engineer acknowledges alert within 5 minutes
    - Perform initial verification to confirm alert is not a false positive
    - Create incident ticket with alert details and initial assessment
    - Tag incident with appropriate component and alert identifier

#### 14.1.2 User-Reported Incident Procedure

1. **Help Desk Call Handling:**
    - Answer all calls within 60 seconds (target 80%)
    - Authenticate caller using established verification protocol
    - Collect essential information:
        - User name, role, and contact information
        - Affected system component or functionality
        - Detailed description of the issue
        - Date/time when issue was first observed
        - Impact on operations (number of users affected, criticality)

        - Steps to reproduce (if known)
        - Screenshots or error messages (if available)
    - Determine if issue is already known (check existing incidents)
2. **In-App Feedback Processing:**
    - Monitor in-app feedback queue in real-time during business hours
    - Review feedback within 30 minutes of submission
    - Contact user for additional details if necessary
    - Create incident ticket for actionable feedback or support requests
    - Route feature requests to Product Management
3. **Email Support Request Handling:**
    - Acknowledge all support emails within 1 hour during business hours
    - Create incident ticket with all relevant details
    - Request additional information if submission is incomplete
    - Provide ticket number to submitter for reference

## 14.2 Incident Classification and Prioritization SOP

#### 14.2.1 Categorization Procedure

1. **Incident Type Classification:**
    - Select primary incident category from standard taxonomy:
        - Hardware Issue (GPS device, ID reader, network equipment)
        - Software Issue (application error, bug, functionality failure)
        - Performance Issue (slow response, timeout, degradation)
        - Data Issue (data quality, missing data, synchronization error)
        - Access Issue (login failure, permission problem)
        - Security Issue (potential breach, vulnerability)
        - Integration Issue (data exchange failure with external systems)
        - User Knowledge Issue (training need, documentation question)
    - Select specific component affected (e.g., Driver Module, Routing Engine, Parent App, School Portal, Admin Console, etc.)
    - Tag with specific error code or message if applicable

2. **User Impact Assessment:**
    - Determine scope of impact:
        - Individual user
        - User group (e.g., specific school, specific SBC)
        - Functionality (e.g., route planning, student check-in)
        - Geographic area
        - System-wide
    - Document number of affected users (estimated or actual)
    - Note any safety implications

#### 14.2.2 Prioritization Matrix Application

1. **Impact Assessment:**

| Impact Level | Definition |
|---|---|
| 1 - Critical | System-wide impact; affects critical transportation operations; safety implications |
| 2 - High | Major function unavailable; affects multiple schools/routes; significant operational disruption |
| 3 - Medium | Limited impact; affects small group of users; workaround available |
| 4 - Low | Minimal impact; affects single user; easy workaround available |

2. **Urgency Assessment:**

| Urgency Level | Definition |
|---|---|
| 1 - Critical | Immediate resolution required; active transportation operations affected; executive visibility |
| 2 - High | Same-day resolution required; significant user frustration; affects time-sensitive operations |
| 3 - Medium | Resolution needed within 2-3 days; moderate user frustration |
| 4 - Low | Resolution can be scheduled; limited or no time sensitivity |

3. **Priority Calculation:**

| | Impact 1 | Impact 2 | Impact 3 | Impact 4 |
|---|---|---|---|---|
| **Urgency 1** | P1 | P1 | P2 | P3 |
| **Urgency 2** | P1 | P2 | P3 | P3 |
| **Urgency 3** | P2 | P3 | P3 | P4 |
| **Urgency 4** | P3 | P3 | P4 | P4 |

4. **Priority Assignment:**
    - Assign initial priority based on matrix calculation
    - Escalate assignment to supervisor for verification if P1 or P2
    - Document justification for priority in ticket notes
    - Set SLA clock based on assigned priority

## 14.3 Tier 1 Support Resolution SOP

#### 14.3.1 Initial Diagnosis Procedure

1. **Knowledge Base Consultation:**
    - Search knowledge base for known issues matching incident symptoms
    - Review FAQs and solution articles related to affected component
    - Check recent release notes for known bugs or changes
2. **Basic Troubleshooting Steps:**
    - Request user perform basic client-side troubleshooting:
        - Browser refresh/cache clearing
        - Application restart
        - Device reboot (for mobile app issues)
        - Alternative browser/device test if applicable
    - Verify user credentials and permissions
    - Check for recent changes to user's account or configuration
    - Verify network connectivity for device-related issues
3. **Remote Assistance:**
    - Offer remote session for desktop/web application issues
    - Guide user through screen sharing if needed

- Document observed behavior during remote session

#### 14.3.2 Common Issue Resolution Procedures

1. **Account Access Issues:**
   - Verify user identity following security protocol
   - Reset password following account management procedure
   - Verify account is not locked or disabled
   - Check for correct user role assignment
   - Validate multi-factor authentication setup if applicable
2. **Mobile App Issues:**
   - Verify app version matches latest release
   - Guide through app update if needed
   - Check device compatibility and OS version
   - Clear app cache and data
   - Reinstall application if necessary
3. **GPS Device Issues:**
   - Verify device power and connectivity
   - Guide through device restart procedure
   - Check signal strength and satellite acquisition
   - Verify device registration in system
   - Schedule field service if hardware issue confirmed

#### 14.3.3 Escalation Procedure

1. **Escalation Criteria:**
   - Issue not resolved after 15 minutes of active troubleshooting
   - Known issue requiring Tier 2 intervention
   - P1/P2 priority incidents requiring immediate technical expertise
   - Issue outside of Tier 1 scope (complex configuration, backend issue)
2. **Escalation Process:**
   - Document all troubleshooting steps taken

- Select appropriate Tier 2 assignment group based on affected component
- Transfer all collected diagnostic information
- Set ticket status to "Escalated"
- Provide estimated response time to user
- For P1/P2: Place direct call to Tier 2 on-call resource

## 14.4 Tier 2 Technical Support SOP

### 14.4.1 In-Depth Technical Analysis Procedure

1. **Ticket Review and Acknowledgment:**
   - Review full incident history and Tier 1 troubleshooting steps
   - Acknowledge ticket within SLA timeframe
   - Update ticket status to "In Progress"
   - Contact user for additional information if needed
2. **Advanced Diagnostic Activities:**
   - Access system logs relevant to affected component
   - Review error messages and stack traces
   - Check recent changes or deployments that might impact the component
   - Analyze database queries and performance metrics
   - Conduct network traffic analysis if applicable
   - Test in staging environment to attempt reproduction
3. **Specialized Component Analysis:**
   - For Routing Engine issues:
     - Analyze optimization parameters and constraints
     - Check for data quality issues in route inputs
     - Verify algorithm version and configuration
   - For Mobile App issues:
     - Review API call failures and response codes
     - Check for device-specific compatibility issues
     - Analyze offline mode synchronization logs

- For Integration issues:
    - Validate data format and structure
    - Check authentication and authorization credentials
    - Verify endpoint availability and connectivity

#### 14.4.2 Resolution Implementation Procedure

1. **Solution Development:**
    - Identify potential fixes or workarounds based on diagnosis
    - Test proposed solution in non-production environment
    - Document step-by-step resolution procedure
    - Assess potential impact of implementing the solution
2. **Change Management Integration:**
    - For configuration changes:
        - Follow standard change process
        - Submit change request with detailed implementation plan
        - Obtain necessary approvals based on change type
        - Schedule implementation during appropriate window
    - For emergency changes (P1/P2):
        - Follow expedited change approval process
        - Document business justification
        - Obtain verbal approval from change authority
        - Implement with appropriate oversight
3. **Solution Implementation:**
    - Execute approved changes following documented procedure
    - Verify solution resolves the incident
    - Document exact changes made in ticket
    - Update configuration management database if applicable

#### 14.4.3 Tier 3 Escalation Procedure

1. **Escalation Criteria:**

- Complex issue requiring code-level changes
- Problem requiring architectural expertise
- Critical performance issues not resolvable through configuration
- Security vulnerability requiring expert analysis
- Unresolved P1/P2 incidents after 2 hours of investigation

2. **Escalation Process:**
    - Document comprehensive diagnostic findings
    - Prepare technical summary of troubleshooting steps
    - Identify specific Tier 3 expertise needed
    - Update ticket and assign to appropriate Tier 3 queue
    - For P1/P2: Direct contact with Tier 3 resource via phone
    - Participate in handoff call if required

## 14.5 Tier 3 Specialist Support SOP

#### 14.5.1 Expert Analysis Procedure

1. **Ticket Review and Expert Assembly:**
    - Analyze complete incident history and previous troubleshooting
    - Assemble appropriate specialist team based on issue domain
    - Establish dedicated communication channel if needed
    - Define investigation approach and required resources
2. **Advanced Technical Investigation:**
    - Access development environments and tools
    - Review source code related to affected components
    - Conduct deep performance analysis (profiling, tracing)
    - Analyze system architecture for potential design issues
    - Conduct memory analysis and thread dumps if applicable
    - Perform database schema and query optimization analysis
3. **Vendor Coordination (if applicable):**
    - Prepare comprehensive issue documentation for vendor support
    - Open vendor support ticket following established procedure

- Coordinate joint debugging sessions if required
- Validate vendor-provided solutions before implementation

#### 14.5.2 Permanent Solution Development

1. **Root Cause Analysis:**
   - Identify underlying root cause through systematic analysis
   - Document causal factors and contributing conditions
   - Assess potential impact on other system components
   - Determine if issue affects multiple environments
2. **Solution Engineering:**
   - Design comprehensive solution addressing root cause
   - Develop code fixes or configuration changes
   - Create detailed technical specification
   - Review solution with architectural team if significant
   - Develop automated tests to verify fix
3. **Release Management Integration:**
   - For emergency patches:
     - Follow expedited review and testing process
     - Create deployment package
     - Schedule emergency release window
     - Obtain necessary approvals
   - For standard releases:
     - Submit code to regular development workflow
     - Tag for inclusion in next release cycle
     - Document thoroughly for release notes

### 14.6 Major Incident Management SOP

#### 14.6.1 Major Incident Declaration and Setup

1. **Incident Declaration:**
   - On-call support supervisor evaluates incident against P1/P2 criteria

- Formally declares Major Incident status
- Designates Major Incident Manager (MIM)
- Creates dedicated incident room in collaboration platform
- Establishes conference bridge

2. **Team Assembly:**
   - MIM activates Major Incident Response Team
   - Sends notifications via alerting system
   - Assembles technical experts based on affected components
   - Designates roles:
     - Technical Lead
     - Communications Coordinator
     - Resolver Groups
     - NYCPS Liaison

3. **Initial Assessment:**
   - Conduct rapid impact analysis
   - Document current status and affected services
   - Establish timeline of events
   - Create initial situation report
   - Determine initial response strategy

#### 14.6.2 Major Incident Coordination Procedure

1. **MIM Responsibilities:**
   - Facilitate regular status calls (every 30 minutes for P1, hourly for P2)
   - Track action items and assignments
   - Remove obstacles to resolution
   - Manage escalations
   - Ensure communication flow to all stakeholders
   - Document key decisions and milestones

2. **Technical Response Activities:**
   - Conduct parallel investigation tracks if needed

- Prioritize service restoration over root cause analysis
- Consider temporary workarounds to restore service
- Test proposed solutions in isolation when possible
- Prepare rollback plans for all changes

3. **Communication Protocol:**
    - Provide regular updates via established channels
    - Create and update status page entry
    - Send email notifications at key milestones
    - Prepare user communication for approved distribution
    - Document timeline of communication activities

#### 14.6.3 Major Incident Resolution and Closure

1. **Service Restoration:**
    - Implement approved solution
    - Verify restoration across all affected components
    - Conduct validation testing
    - Collect confirmation from affected user representatives
    - Monitor for stability for minimum 30 minutes

2. **Incident Closure:**
    - MIM declares service restored
    - Send final status update to all stakeholders
    - Update incident ticket with comprehensive resolution details
    - Document lessons learned in real-time
    - Schedule Post-Incident Review

3. **Transition to Problem Management:**
    - Create problem record linked to incident
    - Transfer key diagnostic information
    - Assign initial investigation team
    - Schedule initial problem analysis meeting

## 14.7 Hardware Support SOP

#### 14.7.1 Hardware Issue Diagnosis

1. **Remote Diagnostics:**
    - Verify device registration and connectivity status
    - Run remote diagnostic tests when possible
    - Review device error logs and alert history
    - Attempt remote reset/restart procedures
    - Check firmware version and update history
2. **Issue Classification:**
    - Categorize as software, firmware, configuration, or hardware failure
    - Determine if issue is:
        - Remotely resolvable
        - Requiring on-site service
        - Requiring device replacement
    - Assign appropriate priority based on operational impact

#### 14.7.2 On-Site Service Procedure

1. **Service Scheduling:**
    - Contact SBC to arrange service appointment
    - Assign field technician based on location and expertise
    - Prepare service order with:
        - Device details and serial number
        - Issue description
        - Diagnostic history
        - Required parts and tools
        - Contact information
    - Confirm appointment 24 hours in advance
2. **On-Site Activities:**
    - Technician arrives within scheduled window
    - Performs physical inspection of device

- Conducts diagnostic tests following standard protocol
- Attempts repair using approved procedures
- Replaces device if repair not possible
- Configures replacement device
- Verifies proper operation before departure

3. **Service Documentation:**
   - Record all actions taken
   - Document parts replaced
   - Update asset management system
   - Obtain sign-off from on-site contact
   - Update ticket with resolution details
   - Trigger RMA process for defective equipment

## 14.8 Post-Incident Review SOP

#### 14.8.1 PIR Preparation

1. **Data Collection:**
   - Compile complete incident chronology
   - Gather system logs covering incident period
   - Collect monitoring data and alerts
   - Document all actions taken during incident
   - Record impact metrics (users affected, duration, etc.)
   - Calculate SLA compliance/breach details

2. **Meeting Scheduling:**
   - Schedule PIR within 3-5 business days of resolution
   - Invite all key participants:
     - Major Incident Manager
     - Technical experts involved in resolution
     - Team leaders from support tiers
     - NYCPS stakeholders
     - Problem Management representative

- Distribute incident summary 24 hours before meeting
- Prepare meeting agenda and framework

#### 14.8.2 PIR Meeting Procedure

1. **Meeting Structure:**
    - Introduce participants and roles
    - Review incident timeline and key events
    - Analyze detection and initial response
    - Evaluate diagnosis and troubleshooting approach
    - Review resolution and recovery actions
    - Assess communication effectiveness
    - Identify root causes and contributing factors
    - Brainstorm preventative measures
2. **Action Item Development:**
    - Document agreed improvement actions
    - Assign specific owners to each action
    - Set concrete deadlines
    - Define success criteria for each action
    - Establish follow-up mechanisms

#### 14.8.3 PIR Documentation and Follow-up

1. **PIR Report Creation:**
    - Document complete incident summary
    - Include timeline with key events
    - Detail root cause analysis findings
    - List all action items with owners and deadlines
    - Highlight systemic issues identified
    - Document lessons learned
2. **Report Distribution:**
    - Distribute report within 48 hours of PIR meeting

- Send to all meeting participants
- Provide copies to management team
- Submit formal copy to NYCPS stakeholders

3. **Action Tracking:**
    - Enter all actions into tracking system
    - Schedule regular status reviews
    - Report progress to stakeholders monthly
    - Validate completed actions for effectiveness
    - Close loop on all identified improvements