STANDARD OPERATING PROCEDURE

IT Incident Management SOP

Document no.	SOP-IT-002
Revision	1.0
Owner	IT Service Delivery Manager
Effective date	September 15, 2026
Review cycle	Every 12 months

1. Purpose

To restore normal IT service as quickly as possible after an unplanned interruption or degradation, with consistent classification, escalation and communication to affected users.

2. Scope

Applies to incidents reported through the ticketing system, phone or monitoring alerts, from detection through resolution and closure. Standard change requests and planned maintenance are covered by the change management SOP.

Definitions

Incident	An unplanned interruption to an IT service or a reduction in its quality.
Severity level	A rating of an incident's business impact and urgency that determines its priority and response.
Major incident	A high-severity incident affecting many users or a critical system, requiring dedicated coordination.
Known error	A documented root cause and workaround for a previously identified problem.

3. Responsibilities

Service Desk Analyst	Logs, classifies and attempts first-line resolution of incidents, and confirms resolution with the user.
Incident Manager	Declares and coordinates major incidents and manages stakeholder communication.
System Administrator	Diagnoses root cause and implements fixes for escalated incidents.
End User	Reports the incident with relevant details and confirms whether the resolution worked.

RACI matrix

Activity	Service Desk Analyst	Incident Manager	System Administrator	End User
Log and classify the incident	R/A	I	I	C
Investigate and resolve the incident	C	I	R/A	I
Declare and manage a major incident	C	R/A	R	I

Activity	Service Desk Analyst	Incident Manager	System Administrator	End User
Communicate status updates	C	R/A	I	I
Confirm resolution and close the ticket	R/A	I	I	C

R = Responsible, A = Accountable, C = Consulted, I = Informed

4. Materials and PPE

Materials, tools and systems

- Ticketing system
- Monitoring and alerting tool
- Known error database or knowledge base
- Severity and priority matrix
- Major incident bridge call or chat channel
- Escalation contact list

5. Procedure

Step	Task	Owner	Done
5.1	**Log the incident** The Service Desk Analyst logs a ticket capturing the reporter, affected system, symptoms and the time the incident was detected, whether reported by a user or a monitoring alert.	Service Desk Analyst	☐
5.2	**Classify severity and priority** The Service Desk Analyst assigns a severity level using the severity and priority matrix, based on business impact and urgency rather than how upset the reporter sounds. **Checkpoint:** The assigned severity matches the criteria in the matrix for the number of users and systems affected.	Service Desk Analyst	☐
5.3	**Check for a known error** The Service Desk Analyst searches the known error database and knowledge base for a documented fix or workaround matching the symptoms before doing new diagnosis.	Service Desk Analyst	☐
5.4	**Attempt first-line resolution** The Service Desk Analyst applies the documented fix or workaround, if one exists, and confirms with the user whether the issue is resolved.	Service Desk Analyst	☐
5.5	**Escalate to second-line support** If the issue is not resolved at first line, the Service Desk Analyst escalates the ticket to the System Administrator with full notes on what was tried and the results.	Service Desk Analyst	☐
5.6	**Declare a major incident if warranted** The Incident Manager declares a major incident when the severity matrix criteria for wide impact or a critical system are met, and opens a communication bridge for the response team. **Warning:** Delaying a major incident declaration to avoid the coordination overhead usually makes the outage last longer.	Incident Manager	☐
5.7	**Diagnose the root cause** The System Administrator investigates logs, recent changes and system health to identify the root cause of the incident.	System Administrator	☐

Step	Task	Owner	Done
5.8	**Implement and test a fix** The System Administrator implements a fix or workaround and tests that the affected service is restored before informing the Service Desk Analyst. **Checkpoint:** The fix is verified against the reported symptoms, not just deployed, before the incident is treated as resolved.	System Administrator	☐
5.9	**Communicate status updates** For major incidents, the Incident Manager sends status updates to affected users and stakeholders at the intervals agreed at the start of the incident.	Incident Manager	☐
5.10	**Confirm resolution with the user** The Service Desk Analyst contacts the original reporter or affected users to confirm the service is working as expected before closing the ticket. **Checkpoint:** The ticket is not closed until the reporter confirms the issue is actually resolved.	Service Desk Analyst	☐
5.11	**Document root cause and resolution** The System Administrator records the root cause, the fix applied and any follow-up work needed in the incident ticket.	System Administrator	☐
5.12	**Close the ticket** The Service Desk Analyst closes the incident ticket once resolution is confirmed and documentation is complete.	Service Desk Analyst	☐
5.13	**Hold a post-incident review** For major incidents, the Incident Manager runs a post-incident review with the response team to capture lessons learned and follow-up actions.	Incident Manager	☐

6. Quality checks

- Every incident ticket records severity, root cause and confirmed resolution before closure.
- Major incidents receive an assigned Incident Manager and a communication bridge promptly after declaration.
- Tickets are not closed without the reporter confirming the service is restored.
- Root cause is documented for every major incident before the ticket is closed.

7. Records

- Incident ticket with classification and resolution
- Root cause documentation
- Post-incident review notes
- Major incident communication log

8. KPIs

- Mean time to resolve by severity level
- Percentage of incidents resolved within the target timeframe for their severity
- Number of major incidents per month
- First-contact resolution rate

9. Common mistakes

- Under-classifying severity to avoid triggering escalation.
- Closing a ticket without confirming the fix with the affected user.
- Skipping the known error check and re-diagnosing an issue that already has a documented fix.

- Not documenting root cause before closing a major incident.

10. Revision history

Revision	Date	Description	Reviewed by
1.0	September 15, 2026	Initial release	Ilia Pirozhenko

Approval

Prepared by	Approved by	Date

This is a template. Adapt it to your organization, equipment and local regulations before use.