

Technical Incident Management and Escalation Protocol

Document ID: IE-IMP-2025.01

Version: 1.0

Effective Date: 2025-11-01

Department: IT & Engineering - DevOps

1. Scope and Objective

This protocol defines the structure and process for responding to, managing, and resolving technical incidents that negatively impact the stability, performance, or security of the NexaCore platform.

2. Incident Severity and Priority

Severity	Definition (Impact)	RTO Target	Escalation (Immediate Contact)
P0 - Critical	Major service outage; catastrophic data loss; security breach affecting core functionality.	< 30 minutes	On-Call Lead, CTO, Head of Legal.
P1 - High	Significant degradation; major feature unusable; large subset of customers impacted.	< 4 hours	On-Call Lead, Engineering Manager.
P2 - Medium	Minor service degradation; isolated feature failure; impacting only internal teams.	< 1 business day	Engineering Manager.
P3 - Low	Cosmetic issues;	Schedule for next	Assigned to

	non-critical system warnings; documentation error.	sprint.	relevant team.
--	---	---------	----------------

3. Incident Lifecycle

1. **Detection:** Triggered by automated monitoring (P0, P1) or direct user report (P2, P3).
2. **Triage & Declaration:** On-Call Lead validates the impact, assigns severity, and declares the incident.
3. **Communication:** Internal communication is initiated via dedicated incident channel (Slack). External communication (for P0/P1) follows the **Data Breach Incident Response Plan** (if applicable).
4. **Remediation:** Incident Commander directs technical team efforts (triage, diagnosis, fix/rollback).
5. **Resolution:** Service returns to normal.
6. **Post-Mortem:** Mandatory for all P0 and P1 incidents.

4. Post-Mortem Requirement

A full Post-Mortem document must be completed within **48 hours** of resolution. It must be **blameless**, focusing on system and process failures, and include concrete, tracked action items to prevent recurrence.