System Monitoring and Alerting Standard

Document ID: IE-MAS-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: IT & Engineering - DevOps

1. Objective

To provide real-time visibility into the health, performance, and security of the entire platform and ensure timely, actionable alerting for on-call teams.

2. Pillars of Monitoring

- **Logs:** Centralized logging solution required for all application, infrastructure, and security logs (SIEM). Logs must be retained for a minimum of **90 days** for troubleshooting.
- **Metrics:** Continuous collection of system metrics (CPU, Memory, Disk) and application metrics (latency, error rates, throughput) via Prometheus/Grafana or equivalent tool.
- **Traces:** Mandatory distributed tracing for all microservices to enable root cause analysis of complex, multi-service requests.

3. Alerting Philosophy

Alerts must be **actionable, specific, and routed to the correct On-Call Team.**

- **Thresholds:** Alerts must be based on Service Level Objectives (SLOs), focusing on the customer experience (e.g., Latency degradation, Error Rate spike) rather than purely resource utilization (e.g., CPU > 90%).
- **Routing:** Alerts are routed through an automated incident response tool that follows the **Technical Incident Management Protocol** for escalation (P0/P1 alerts must page the On-Call Lead).
- **Silence/Deduplication:** Noise is minimized through smart deduplication and pre-defined silence windows for planned maintenance.

4. Health Checks

All services must expose standard, unauthenticated /health or /metrics endpoints used by load balancers and Kubernetes for readiness and liveness probes.