# Standard Operating Procedure (SOP): Production System Patching

Document ID: OPS-SOP-PATCH-005
Department: Operations (SRE Team)
Version: 2.0
Date: 2025-09-15

## 1. Scope and Objective

This SOP covers the uniform procedure for applying operating system (OS), kernel, and core software patches to all production servers, virtual machines, and base container images. The objective is to maintain security compliance while ensuring zero-downtime service delivery.

## 2. Pre-Patching Requirements

1. **Change Request (CR):** A Normal CR must be submitted and approved by the CAB (unless the patch is a critical emergency security fix (P0)).
2. **Snapshot:** A full snapshot or AMI (Amazon Machine Image) of the target system/base image **MUST** be taken immediately before patching begins.
3. **Runbook Review:** The rollback procedure must be reviewed and confirmed executable (MTTB defined).
4. **Monitoring Check:** All system health checks and alerting must be confirmed operational prior to the window.

## 3. Patching Procedure (Standard Change Window)

1. **Notification:** Post status to the #ops-status Slack channel 30 minutes before starting.
2. **Pilot Patching:** Apply the patch to a single, non-critical 'Canary' instance in the production environment.
3. **Canary Test:** Run a full suite of automated health checks and synthetic user transactions against the Canary instance.
    - *If success:* Proceed to Step 4.
    - *If failure:* Execute rollback on the Canary instance and immediately escalate to P1 incident.
4. **Phased Rollout (Wave 1):** Apply the patch to  of the server pool/cluster nodes.
5. **Observation (15 Minutes):** Monitor key metrics (CPU, Memory, Network, Service Latency). If performance is stable and there are no alerts, proceed to Wave 2.
6. **Phased Rollout (Wave 2):** Apply the patch to the remaining  of the server pool/cluster nodes.
7. **Final Verification:** Run final regression tests on the entire environment.

## 4. Rollback Procedure

If any step in the patching procedure fails or causes a P1/P0 alert:

1. **Halt:** Immediately halt the patching process.
2. **Decide:** Incident Commander determines if the patch is fully rolled back, or if a temporary fix is needed.
3. **Execute:** Deploy the pre-patch snapshot/AMI or revert the base container image tag across the fleet.
4. **Confirm:** Verify the service is stable on the rolled-back version.
5. **Post-Mortem:** A formal P1 post-mortem must be initiated immediately to understand the failure.