

Change Management Policy Example for DevOps Organizations

1. Purpose

This Change Management Policy applies to all changes affecting IT systems, applications, and infrastructure operated by the DevOps team. Its purpose is to ensure changes are implemented with minimal risk and disruption to business operations.

2. Scope

This policy covers all environments (development, staging, production) and applies to software releases, infrastructure modifications, configuration updates, and emergency changes managed by the DevOps organization.

3. Definitions

- Change:** Any modification to IT services, systems, or infrastructure.
- Normal Change:** A standard change that follows the full change management process.
- Emergency Change:** A change that must be implemented immediately to resolve an incident or critical problem.
- Standard Change:** A pre-approved, low-risk, and repetitive change.

4. Change Types

Type	Description	Approval Required
Standard	Routine, low-risk, pre-authorized (e.g., weekly deployment)	Pre-approved
Normal	Non-routine, moderate/high risk	Change Manager, Stakeholders
Emergency	Immediate action required	Ops Manager, Post-review

5. Roles and Responsibilities

- Change Requester:** Initiates the change proposal and provides details.
- DevOps Engineer:** Assesses, implements, and validates the change.
- Change Manager:** Reviews, approves, schedules, and communicates changes.
- Stakeholders:** Informed or consulted depending on potential impact.

6. Change Management Process

- Submit change request in the designated system.
- Evaluate potential risks and impact analysis.
- Obtain the necessary approvals based on change type.
- Schedule and communicate the change window.
- Implement the change following documented procedures.
- Test and validate the outcome.
- Update documentation and communicate completion.
- Review and close the change request.

7. Emergency Changes

- Bypass regular approval for immediate resolution.
- Log and document all actions retrospectively.
- Conduct a post-implementation review.

8. Communication

All stakeholders affected by approved changes must be notified prior to implementation, including the scope, timing, and rollback plan if applicable.

9. Policy Compliance

- Compliance is mandatory for all DevOps staff.
- Non-compliance may result in corrective action.

10. Review and Revision

This policy will be reviewed annually or as needed due to significant organizational or technological changes.