

# Change Management Policy

---

## Purpose

Unplanned or unreviewed changes are a leading cause of outages and security incidents. This policy defines how changes to Your Organization production environments are proposed, reviewed, approved, implemented, and documented, balancing the need for agility with the need for predictability and auditability.

## Scope

This policy applies to all changes affecting Your Organization production systems — application code, infrastructure, configuration, network and security controls, identity configuration, data pipelines, and production data. It applies to every workforce member and third party that initiates or executes such changes.

## Change classifications

Changes are classified on two axes: risk (impact and likelihood of disruption) and urgency (how quickly the change must land).

- **Standard change.** Low-risk, pre-approved change following an established runbook — for example, routine user provisioning or a documented patch. No ticket-by-ticket CAB review; logged for audit.
- **Normal change.** Change with non-trivial risk or user-visible impact. Requires a written change ticket, peer review, and explicit approval from the change owner and an independent reviewer before implementation. Large or cross-team normal changes are reviewed at the Change Advisory Board (CAB).
- **Emergency change.** Unplanned change required to restore service or prevent imminent harm. Can be approved out-of-band by the on-call change owner with a documented phone or chat approval; a full change ticket and post-change review must be filed within one business day.
- **Code deployment.** Application code deploys follow the deploy runbook: merged PR with peer review, CI green, automated deploy with health checks, and a documented rollback path. Deploys are logged; production deploy access is limited to approved roles.

## Change Advisory Board (CAB)

The CAB is the cross-functional group that reviews high-risk or high-impact changes before they ship. Standing membership includes engineering, SRE / infrastructure, security, and product. The CAB meets on a recurring cadence (typically weekly) and on demand for emergency escalation. The CAB reviews:

- Purpose and business justification.
- Risk assessment: what could go wrong, blast radius, affected customers or internal users.
- Testing evidence: pre-production validation, load or security testing where applicable.
- Rollback plan: how the change will be reversed if it fails in production.
- Communications plan: who needs to know before, during, and after.

The CAB approves, defers, or rejects. Approvals record the reviewers and conditions imposed.

## Required elements of every change ticket

- Title and description.
- Change owner (named individual).
- Classification (standard / normal / emergency / deploy).
- Affected systems and data classifications.
- Pre-change state and post-change state.
- Implementation steps.
- Test and validation evidence.
- Rollback plan.
- Communications plan.
- Approval record (who approved, when, and under what conditions).
- Post-change summary (success, issues encountered, any follow-up).

## Segregation of duties

Wherever tooling and team size allow, the individual who *requests* a change is distinct from the individual who *approves* it, and from the individual who *implements* it in production. For small teams where strict separation is infeasible, compensating controls (independent review, enhanced logging, automated policy-as-code checks) apply.

## Access to production

Change implementation uses standing privileged access only when no safer alternative is available. Where supported, just-in-time elevation with approval and automatic revocation is preferred. Production consoles, deploy systems, and break-glass accounts are all logged and reviewed (see the Access Control Policy).

## Emergency changes

The emergency change path is reserved for restoring service, stopping an ongoing incident, or closing an active vulnerability with credible exploit pressure. It is not a shortcut for ordinary work. The on-call approver for emergency changes is the senior engineering leader on call or their designated delegate. Post-change, a normal change ticket, timeline, and root-cause analysis are required within one business day.

## Unauthorized changes

Any change implemented outside this process is an unauthorized change. Unauthorized changes are reverted wherever safe to do so, investigated, logged, and addressed per workforce accountability procedures.

## Scope exceptions

Exceptions must be approved by the CIO or CISO, document compensating controls, and be time-bound.

## Review cadence

This policy is reviewed annually by the CAB chair, the SRE lead, and the security team, or sooner following a significant change-related incident.

*Effective date: [the date this policy takes effect]*