

# CI/CD Pipeline

# CI/CD Pipeline

“ **Project:** {{PROJECT\_NAME}} **Version:** {{VERSION}} **Date:** {{DATE}}  
**Author:** {{AUTHOR}} **Status:** Draft | In Review | Approved **Reviewers:**  
{{REVIEWERS}}

## Document History

Version	Date	Author	Changes
0.1	{{DATE}}	{{AUTHOR}}	Initial draft

## 1. Overview

**CI/CD Platform:** {{PLATFORM}} **Container Registry:** {{REGISTRY}} **Deployment Target:** {{DEPLOY\_TARGET}} **Strategy:** {{STRATEGY}}

## 2. Pipeline Overview

```
flowchart LR
  subgraph Source
    PR[Pull Request]
    MERGE[Merge to main]
  end

  subgraph CI["CI – runs on every PR"]
    LINT[Lint & Format]
    TEST_UNIT[Unit Tests]
  end
```

```
    TEST_INT[Integration Tests]
    SAST[SAST Scan]
    SCA[Dependency Scan]
    BUILD[Build Artifact]
end

subgraph CD_DEV["CD – Dev Auto-Deploy"]
    DEPLOY_DEV[Deploy to Dev]
    SMOKE_DEV[Smoke Tests]
end

subgraph CD_STAGING["CD – Staging (auto on main)"]
    DEPLOY_STG[Deploy to Staging]
    TEST_E2E[E2E Tests]
    PERF[Performance Tests]
end

subgraph CD_PROD["CD – Production (manual gate)"]
    APPROVAL[Manual Approval]
    DEPLOY_PROD[Deploy to Production]
    SMOKE_PROD[Smoke Tests]
    MONITOR[Verify Monitoring]
end

PR --> LINT
LINT --> TEST_UNIT
TEST_UNIT --> TEST_INT
TEST_INT --> SAST
SAST --> SCA
SCA --> BUILD
MERGE --> CD_DEV
BUILD --> DEPLOY_DEV
DEPLOY_DEV --> SMOKE_DEV
SMOKE_DEV --> DEPLOY_STG
DEPLOY_STG --> TEST_E2E
TEST_E2E --> PERF
PERF --> APPROVAL
APPROVAL --> DEPLOY_PROD
DEPLOY_PROD --> SMOKE_PROD
SMOKE_PROD --> MONITOR
```

# 3. Source Control Configuration

## 3.1 Branching Strategy

**Strategy:** `{{BRANCH_STRATEGY}}`

Branch	Purpose	Naming Convention	Lifetime
<code>main</code>	Production-ready code	fixed	Permanent
<code>develop</code>	Integration branch	fixed	Permanent
<code>feature/*</code>	New features	<code>feature/{{TICKET}}-description</code>	Until merged
<code>fix/*</code>	Bug fixes	<code>fix/{{TICKET}}-description</code>	Until merged
<code>hotfix/*</code>	Production hotfixes	<code>hotfix/{{TICKET}}-description</code>	Until merged
<code>release/*</code>	Release preparation	<code>release/v{{VERSION}}</code>	Until merged

## 3.2 Branch Protection Rules

**Protected Branches:** `main`, `develop`

Rule	<code>main</code>	<code>develop</code>
Require PR	Yes	Yes
Required approvals	<code>{{APPROVALS}}</code>	1
Dismiss stale reviews	Yes	Yes
Require status checks	Yes	Yes
Required checks	lint, unit-tests, integration-tests, sast	lint, unit-tests
Require up-to-date	Yes	No
Allow force push	No	No
Allow deletions	No	No

## 3.3 Code Review Requirements

- Minimum `{{APPROVALS}}` approval(s) required before merge
- At least one approval from a **code owner** (see `CODEOWNERS`)
- All review comments must be **resolved** before merge

- Review turnaround SLA: `{{REVIEW_SLA}}` business hours
- Auto-assign reviewers via: `{{ASSIGN_MECHANISM}}`

## 4. Build Stage

### 4.1 Build Tool & Configuration

Parameter	Value
Build Tool	<code>{{BUILD_TOOL}}</code>
Build Command	<code>{{BUILD_CMD}}</code>
Artifact Type	<code>{{ARTIFACT}}</code>
Artifact Naming	<code>{{REGISTRY}}/{{IMAGE_NAME}}:{{TAG_STRATEGY}}</code>
Tag Strategy	<code>git-sha</code> for PRs, <code>semver</code> for releases

### 4.2 Dependency Caching

Cache	Key	Restore Keys
Node modules	<code>node-modules-{{OS}}-{{LOCKFILE_HASH}}</code>	<code>node-modules-{{OS}}</code>
Docker layers	<code>buildx-{{DOCKERFILE_HASH}}</code>	<code>buildx-</code>
Test results	<code>test-results-{{COMMIT_SHA}}</code>	N/A

### 4.3 Artifact Generation

Artifact	Storage	Retention	Signed
Docker image	<code>{{REGISTRY}}</code>	90 days (non-prod), Forever (prod tags)	<code>{{SIGNING}}</code>
Test reports	CI artifact storage	30 days	No
SBOM	<code>{{SBOM_STORAGE}}</code>	1 year	Yes
Coverage report	<code>{{COVERAGE_STORAGE}}</code>	30 days	No

## 5. Test Stages

## 5.1 Unit Tests

Parameter	Value
Framework	{{UNIT_FRAMEWORK}}
Command	{{UNIT_CMD}}
Coverage Tool	{{COVERAGE_TOOL}}
Coverage Gate	≥ {{COVERAGE_GATE}}% lines, ≥ {{BRANCH_GATE}}% branches
Failure Action	Block PR merge

## 5.2 Integration Tests

Parameter	Value
Framework	{{INT_FRAMEWORK}}
Command	{{INT_CMD}}
Dependencies	{{INT_DEPS}}
Failure Action	Block PR merge

## 5.3 E2E Tests

Parameter	Value
Framework	{{E2E_FRAMEWORK}}
Command	{{E2E_CMD}}
Environment	Staging
Parallelization	{{E2E_SHARDS}} shards
Failure Action	Block staging promotion

## 5.4 Security Scanning

Scan Type	Tool	Command	Gate
SAST	{{SAST_TOOL}}	{{SAST_CMD}}	Block on HIGH/CRITICAL
SCA (dependencies)	{{SCA_TOOL}}	{{SCA_CMD}}	Block on CRITICAL
Container scan	{{CONTAINER_SCAN}}	{{CONTAINER_SCAN_CMD}}	Block on CRITICAL
Secret scanning	{{SECRET_SCAN}}	{{SECRET_SCAN_CMD}}	Block on any finding

## 5.5 Linting & Formatting

Tool	Purpose	Command	Auto-fix
{{LINTER}}	Code linting	{{LINT_CMD}}	PR comment
{{FORMATTER}}	Code formatting	{{FMT_CMD}}	Auto-commit or fail
{{TYPE_CHECK}}	Type checking	{{TYPE_CMD}}	No

# 6. Deploy Stages

## 6.1 Deployment Strategy

**Strategy:** {{DEPLOY\_STRATEGY}}

**Rolling Deployment:**

- Batch size: {{BATCH\_SIZE}}% of instances
- Pause between batches: {{PAUSE}}min
- Health check wait: {{HEALTH\_WAIT}}s
- Rollback trigger: health check failure

**Canary Deployment (if used):**

- Initial canary weight: {{CANARY\_INITIAL}}%
- Increment: {{CANARY\_INCREMENT}}% every {{CANARY\_INTERVAL}}min
- Promotion criteria: error rate < {{ERROR\_THRESHOLD}}%, p99 < {{LATENCY\_THRESHOLD}}ms
- Rollback trigger: automatic on threshold breach

## 6.2 Environment Promotion

PR Branch → Dev (auto) → Staging (auto on main merge) → Production (manual approval)

Promotion	Trigger	Gate	Approver
→ Dev	Merge to <code>develop</code> / PR	All CI checks pass	Automatic
→ Staging	Merge to <code>main</code>	All CI + Dev smoke tests	Automatic
→ Production	Tag <code>v*.*.*</code>	All tests + manual approval	{{PROD_APPROVER}}

## 6.3 Approval Gates

**Production Approval Required:** Yes **Approvers:** `{{PROD_APPROVERS}}` (at least `{{APPROVAL_COUNT}}` required) **Approval Window:** `{{APPROVAL_WINDOW}}`h (pipeline cancels after timeout) **Emergency Override:** `{{EMERGENCY_OVERRIDE}}`

## 6.4 Feature Flags Integration

**Feature Flag Tool:** `{{FF_TOOL}}` **Flag Validation:** Feature flags validated in staging before production deploy **Kill Switch:** All new features behind flags for first `{{FF_PERIOD}}` days

---

# 7. Post-Deploy

## 7.1 Smoke Tests

Check	Expected	Timeout
Health endpoint <code>GET /health</code>	HTTP 200	10s
Auth endpoint reachable	HTTP 401	10s
Database connection	Healthy	15s
Cache connection	Healthy	10s
Critical user journey	Success	60s

**Smoke test timeout:** `{{SMOKE_TIMEOUT}}`min total **On failure:** Auto-rollback triggered

## 7.2 Monitoring Verification

Metric	Threshold	Check Duration
Error rate	< <code>{{ERROR_RATE}}</code> %	5 min
P99 latency	< <code>{{P99}}</code> ms	5 min
CPU utilization	< <code>{{CPU}}</code> %	5 min
Memory utilization	< <code>{{MEM}}</code> %	5 min

## 7.3 Rollback Triggers

**Automatic rollback triggers:**

- Smoke test failure
- Error rate > `{{AUTO_ROLLBACK_ERROR}}`% for `{{AUTO_ROLLBACK_DURATION}}`min post-deploy
- Health check failure on `{{HEALTH_FAIL_THRESHOLD}}`% of instances

**Manual rollback:** See [rollback-plan.md](#)

## 8. Pipeline Configuration Reference

**Config File Location:** `{{CONFIG_PATH}}`

Key environment variables injected by CI:

Variable	Source	Purpose
<code>REGISTRY_TOKEN</code>	<code>{{SECRET_STORE}}</code>	Container registry auth
<code>DEPLOY_KEY</code>	<code>{{SECRET_STORE}}</code>	Deployment credentials
<code>SENTRY_DSN</code>	<code>{{SECRET_STORE}}</code>	Error tracking
<code>SLACK_WEBHOOK</code>	<code>{{SECRET_STORE}}</code>	Notifications

## 9. Secret Injection Strategy

**Strategy:** `{{SECRET_STRATEGY}}`

Secret Type	Storage	Injection Method	Rotation
Registry credentials	<code>{{STORAGE}}</code>	<code>{{METHOD}}</code>	<code>{{ROTATION}}</code>
Cloud credentials	<code>{{STORAGE}}</code>	OIDC / Workload Identity	Per-job
App secrets	<code>{{STORAGE}}</code>	<code>{{METHOD}}</code>	<code>{{ROTATION}}</code>

**OIDC Preferred:** Cloud credentials injected via OIDC — no long-lived keys stored in CI

## 10. Pipeline Metrics

Metric	Target	Current
Build duration (P50)	< <code>{{BUILD_TARGET}}</code> min	TBD

Metric	Target	Current
Test duration (P50)	< {{TEST_TARGET}}min	TBD
Total pipeline duration	< {{TOTAL_TARGET}}min	TBD
Deploy frequency	{{DEPLOY_FREQ}}	TBD
Lead time for changes	< {{LEAD_TIME}}	TBD
Change failure rate	< {{FAILURE_RATE}}%	TBD
MTTR	< {{MTTR}}	TBD

## Related Documents

- [Deployment Architecture](#)
- [Environment Configuration](#)
- [Deployment Checklist](#)
- [Rollback Plan](#)
- [Test Strategy](#)

## Approval

Role	Name	Date	Signature
Author			
Reviewer			
Approver			

Revision #7

Created 2026-02-23 13:16:36 UTC by John

Updated 2026-05-25 07:33:45 UTC by John