DevSecOps Pipeline Review Template

BhanuReddy.cloud | Cloud Security Consulting

Source and Secrets

[ ] Default branches should require pull request review before merge.

[ ] Branch protection should prevent direct pushes to production branches.

[ ] Secrets scanning should run on pull requests and default branches.

[ ] Detected secrets should trigger rotation and incident review workflows.

[ ] Repository deploy keys and tokens should be scoped to least privilege.

[ ] Inactive users and stale repository access should be removed.

Application and IaC Scanning

[ ] SAST should run on pull requests for supported application languages.

[ ] DAST should be used for internet-facing applications where practical.

[ ] Dependency scanning should detect vulnerable libraries and packages.

[ ] Infrastructure-as-code scanning should run for Terraform, CloudFormation, Kubernetes manifests or Helm charts.

[ ] Critical and high findings should have documented triage ownership.

[ ] False-positive exceptions should expire and require justification.

Build and Container Security

[ ] Container image scanning should run before images are promoted.

[ ] Images should avoid running as root where possible.

[ ] Base images should be pinned, maintained and reviewed for vulnerabilities.

[ ] Container images should not use the latest tag for production releases.

[ ] SBOMs should be generated for release artifacts.

[ ] Build artifacts should be stored in approved registries or artifact repositories.

DevSecOps Pipeline Review Template

Artifact Integrity and Release Gates

[ ] Release artifacts should be signed where supported.

[ ] Build provenance should be traceable from source commit to deployed artifact.

[ ] Critical vulnerabilities should block release unless an approved exception exists.

[ ] Production deployments should require approval from authorized owners.

[ ] Security gates should have documented severity thresholds.

[ ] Emergency release bypasses should be logged and reviewed.

Cloud Deployment Controls

[ ] Pipeline IAM roles should follow least privilege.

[ ] Production deployment roles should be separated from development roles.

[ ] Long-lived cloud credentials should not be stored in CI/CD variables where federation is available.

[ ] Deployment logs should be retained for investigation and audit evidence.

[ ] Environment variables should not expose secrets in build logs.

[ ] Cloud changes should be traceable to a commit, workflow run and approver.

Operations and Ownership

[ ] Security findings should have assigned owners and remediation due dates.

[ ] Pipeline failures should notify the responsible team.

[ ] Security tools should be tuned to reduce recurring low-value noise.

[ ] Remediation guidance should be available for common finding types.

[ ] Metrics should track critical findings, exception count and time to remediate.

[ ] Pipeline security controls should be reviewed after major architecture changes.