CI/CD Pipeline Security Checklist

Pipeline hardening and supply chain protection

Pipeline Configuration

- ■ Pipeline definitions stored in version control (not UI-only)
- ■ Pipeline changes require code review approval
- ■ Runners/agents isolated (ephemeral containers preferred)
- ■ Network egress from runners restricted to necessary endpoints

Secrets Management

- ■ Secrets injected via CI secrets manager (not environment files)
- ■ Secrets scoped to minimum required pipelines/environments
- ■ No secrets printed in build logs (masking enabled)
- ■ Secrets rotated on a defined schedule

Artifact Integrity

- ■ Build artifacts signed with verified keys
- ■ SBOM generated for every release build
- ■ Artifact registry access controlled and audited
- ■ Dependency pinning with hash verification enabled