

# Code Testing and Deployment Policy

This document outlines our organization's enforcement of code testing before deployment to production assets.

1. **\*\*Pre-Deployment Testing Enforcement\*\*** - All code changes must pass through automated testing pipelines (unit, integration, and regression tests). - Manual code reviews are required for critical features or security-related changes. - Staging environment testing is mandatory before deployment to production.
2. **\*\*CI/CD Pipeline Enforcement\*\*** - Continuous Integration (CI) is enforced to run test suites automatically on every commit. - Deployment to production is gated and only possible if all automated tests pass successfully. - Failed tests block the deployment pipeline until resolved.
3. **\*\*Approval Process\*\*** - Deployment requires approval from at least one senior engineer or administrator after test results are validated. - Rollback procedures are documented and available in case post-deployment issues arise.
4. **\*\*Monitoring and Reporting\*\*** - Test coverage reports are generated and monitored to ensure quality standards are met. - Deployment logs are stored for auditing and compliance purposes.

This ensures that all code changes undergo logical and enforced testing prior to production deployment, minimizing risk and ensuring system stability.