ALTNETIX LLC
VitaAI Platform

CHANGE MANAGEMENT WORKFLOW

Software Development and Production Change Control Process

Control Reference	PDP-7
Document Version	1.0
Effective Date	June 1, 2026
Next Review	June 1, 2027
Classification	Confidential – Internal & Customer Use
Maintained by	Altnetix LLC Security & Compliance Team
Contact	compliance@altnetix.com

1. Purpose and Scope

This Change Management Workflow governs all changes to production systems, including the VitaAI API, frontend application, Azure infrastructure, database schemas, and security configurations. All changes — regardless of size — must follow this process to ensure stability, security, and auditability.

2. Change Categories

Category	Description	Examples	Approval Required
Standard	Pre-approved routine changes with low risk	Dependency updates, minor UI fixes	Team Lead review
Normal	Planned changes requiring review and testing	New features, schema migrations	Security + Peer review
Emergency	Urgent fixes for critical production issues	Security patches, P0 bug fixes	CEO + Security Officer

3. Change Request Process

All changes originate as a work item in Azure DevOps. The change author must document: description of change, impacted systems, rollback procedure, test plan, and security impact assessment. Changes touching authentication, PHI storage, or cryptographic controls require Security Officer review.

4. Code Review Requirements

- All code changes require peer review by at least one other developer before merging
- Security-sensitive changes (auth, encryption, PHI handling) require Security Officer review
- Code review must verify: functional correctness, OWASP secure coding, test coverage, no secrets in code

- Branch protection rules enforce required reviews before merge to main branch

5. Testing Requirements

- Unit tests must cover all new business logic (>80% coverage target)
- Integration tests required for API endpoint changes
- Database migration scripts must be tested on staging before production
- Security-affecting changes must pass OWASP ZAP or equivalent scan
- Staging environment must validate changes before any production deployment

6. Deployment Process (Azure DevOps)

All production deployments occur via the Azure DevOps CI/CD pipeline:

- Code merged to main branch triggers automated build and test pipeline
- Pipeline deploys to Staging environment for final validation
- Production deployment requires manual approval gate from authorized approver
- Blue-green or slot-swap deployment minimizes downtime
- Deployment is logged with commit SHA, deployer identity, and timestamp in audit trail

7. Post-Deployment Verification

- Application health checks verified within 5 minutes of deployment
- Key transaction flows tested manually or via automated smoke tests
- Azure Monitor / Application Insights reviewed for error rate anomalies
- Rollback initiated if error rate increases >1% above baseline within 30 minutes

8. Emergency Changes

Emergency changes (P0 severity) may bypass standard review timelines but still require: (a) CEO and Security Officer verbal/chat approval, (b) peer review by at least one engineer, (c) immediate post-deployment documentation of the change rationale. HIPAA-impacting emergency changes must be documented within 24 hours.