Change Management Policy

Document ID: COM-INT-010 **Last Updated:** February 2024 **Owner:** IT Operations **Applies To:** All Technical Teams

---

Purpose

This policy establishes the change management process for all changes to NovaTech's production systems and infrastructure. Effective change management reduces risk, prevents outages, and ensures changes are properly reviewed and documented.

Scope

This policy applies to: - Production environment changes - Staging environment changes (expedited process) - Infrastructure changes (network, servers, cloud) - Database changes - Application deployments - Configuration changes - Security changes

Excluded: - Development environment changes - Non-production testing - Documentation-only changes

---

Change Types

Standard Changes

Pre-approved, low-risk changes with established procedures.

Examples: - Routine password rotations - Adding users to existing groups - Deploying previously approved code - Updating monitoring thresholds

Process: No CAB approval required; follow documented procedure.

Normal Changes

Changes requiring review and approval before implementation.

Examples: - New feature deployments - Database schema changes - Infrastructure modifications - New integrations - Configuration changes

Process: Submit change request, CAB review, approval required.

Emergency Changes

Urgent changes to restore service or address security issues.

Examples: - Production outage fixes - Security vulnerability patches - Critical bug fixes - Incident recovery

Process: Expedited approval, post-implementation review.

Change Risk Assessment

Risk Levels

Risk	Impact	Approval	Timing
Low	Minimal, easily reversible	Manager	Anytime
Medium	Moderate, reversible	CAB	Change window
High	Significant, complex rollback	CAB + VP	Change window
Critical	Business-critical, high complexity	CAB + CTO	Scheduled maintenance

Risk Factors

Consider: - Scope of change - Number of systems affected - Reversibility - Customer impact - Compliance implications - Testing level

---

Change Request Process

1. Submit Change Request

Create change request in Jira (Change Management project):

Required Information: - Description of change - Business justification - Risk assessment - Implementation plan - Rollback plan - Testing completed - Estimated duration - Change window requested

2. Review

Technical Review: - Architecture review (if required) - Security review (if required) - Peer review of implementation plan

Manager Approval: - For low-risk changes - Verify completeness - Approve or escalate

3. CAB Review

Change Advisory Board meets: - Tuesday and Thursday at 11 AM CT - Reviews medium+ risk changes - Emergency CAB available 24/7

CAB Members: - IT Operations Manager (chair) - Engineering representative - Security representative - Service owner (for affected systems)

4. Approval

Approval Matrix:

Risk Level	Approvers
Low	Manager
Medium	CAB
High	CAB + VP Engineering
Critical	CAB + CTO

5. Implementation

- Follow approved implementation plan
- Communicate status updates
- Verify successful completion
- Execute rollback if needed

6. Post-Implementation Review

- Verify change objectives met
- Document any issues
- Update documentation
- Close change request

Change Windows

Standard Change Windows

Window	Time (CT)	Use For
Daily	6 AM - 8 AM	Low-risk changes
Nightly	11 PM - 5 AM	Medium-risk changes
Weekend	Sat 2 AM - 6 AM	High-risk changes
Maintenance	Scheduled	Critical changes

Change Freeze Periods

No non-emergency changes during: - Quarter-end (last 3 business days) - Major holidays - Critical customer events - Declared freeze periods

Exceptions: Emergency changes with VP+ approval.

Emergency Change Process

When to Use

- Production outage recovery
- Active security incident
- Critical customer impact
- Regulatory compliance

Process

1. **Notify** on-call manager
2. **Get verbal approval** from authorized approver

3. **Implement change** with available personnel
4. **Document actions** as you go
5. **Submit change request** within 24 hours
6. **Complete post-mortem** if incident-related

Authorized Emergency Approvers

- Director of Engineering or above
- Security Director (security changes)
- On-call incident commander (during active incidents)

Roles and Responsibilities

Change Requester

- Complete change request accurately
- Conduct thorough testing
- Develop rollback plan
- Implement change as approved
- Communicate status

Change Manager

- Facilitate CAB meetings
- Ensure process compliance
- Track change metrics
- Coordinate communications

Change Advisory Board

- Review change requests
- Assess risk
- Approve or reject changes
- Provide implementation guidance

Service Owner

- Approve changes to their service
- Ensure business impact understood
- Coordinate with stakeholders

Documentation Requirements

Change Request

- Clear description
- Business justification
- Technical details
- Risk assessment
- Implementation steps
- Rollback procedure
- Test evidence
- Communication plan

Post-Implementation

- Actual implementation steps
- Issues encountered
- Resolution of issues
- Verification results
- Lessons learned

Communication

Stakeholder Notification

Change Type	Notification	Timing
Low risk	None required	-
Medium risk	Affected teams	24 hours before
High risk	Broader communication	48 hours before
Customer impact	Status page + email	72 hours before

Status Updates

During implementation: - Begin: "#change-notifications channel" - Completion or rollback: Same channel - Issues: Incident process if needed

---

Metrics

Key Metrics

Metric	Target
Change success rate	>95%
Emergency change rate	<10%
Change-related incidents	<5%
CAB meeting frequency	2x/week
Documentation compliance	100%

Reporting

- Weekly change summary
- Monthly change metrics
- Quarterly trend analysis

Compliance

Audit Requirements

- All changes documented
- Approval records maintained
- Implementation evidence captured
- Retain records for 7 years

SOC 2 Alignment

- CC8.1: Change management controls
- Segregation of duties
- Authorization requirements
- Documentation standards

Exceptions

Exception Process

1. Document exception request
2. Justify business need
3. Identify compensating controls
4. VP+ approval required
5. Document approval
6. Time-limited (90 days max)

Training

Required Training

All technical staff: - Change management fundamentals - Change request procedure - Emergency change process

Change Advisory Board: - Risk assessment - CAB procedures

Related Documents

- Incident Management Process (IT-SUP-020)
- Release Management Policy (IT-OPS-020)
- Security Change Policy (IT-SEC-030)
- Database Change Procedures (IT-OPS-025)

Contact

- **Change Management:** change-management@novatech.com
- **Emergency CAB:** emergency-cab@novatech.com
- **Slack:** #change-management

Review Cycle: Annual Next Review: February 2025