🚨 MANDATORY REVIEW POLICY

📋 Policy Overview

CRITICAL: This repository enforces a MANDATORY REVIEW POLICY for all changes. No exceptions are permitted.

Effective Date: September 22, 2025
Policy Status: ✅ **ACTIVE AND ENFORCED**
Compliance: 🔒 **MANDATORY FOR ALL CONTRIBUTORS**

🔒 Core Policy Requirements

1. MANDATORY REVIEW ENFORCEMENT

- **ALL changes require comprehensive CodeRabbit review**
- **NO changes may be merged without complete review approval**
- **Review requirements apply to ALL branches without exception**
- **All contributors must comply with review policy**

2. BRANCH COVERAGE

Mandatory Review Required On:
- `main` branch
- `deploy-training` branch
- `hx-integration` branch
- `repository-restructure` branch
- All feature branches (`feature/*`)
- All fix branches (`fix/*`)
- All hotfix branches (`hotfix/*`)
- All release branches (`release/*`)

3. FILE TYPE COVERAGE

Mandatory Review Required For:
- All Python files (`**/*.py`)
- All documentation (`**/*.md`)
- All configuration files (`**/*.yaml` , `**/*.yml` , `**/*.json`)
- All shell scripts (`**/*.sh`)
- All text files (`**/*.txt`)

🎯 Review Requirements

Code Quality Review - MANDATORY

- Security vulnerability assessment
- Best practices compliance verification

- Error handling and edge case validation
- Performance impact analysis
- Code maintainability evaluation

Documentation Review - MANDATORY

- Markdown formatting validation
- Content accuracy verification
- Link integrity checking
- Heading hierarchy compliance
- Table formatting validation

Testing Review - MANDATORY

- Unit test coverage verification
- Test quality and isolation validation
- Mock and fixture implementation review
- Test documentation completeness
- Integration test effectiveness

Configuration Review - MANDATORY

- YAML/JSON syntax validation
- Configuration completeness verification
- Security configuration assessment
- Environment compatibility checking
- Deployment readiness validation

🚫 PROHIBITED ACTIONS

STRICTLY FORBIDDEN:

- ❌ Merging without CodeRabbit review approval
- ❌ Bypassing review requirements
- ❌ Using emergency merge procedures without authorization
- ❌ Disabling CodeRabbit reviews
- ❌ Modifying review configuration without approval

ENFORCEMENT MECHANISMS:

- Automated review requirement validation
- Branch protection rules enforcement
- Merge blocking for unreviewed changes
- Audit trail maintenance for all reviews
- Compliance monitoring and reporting

✅ Compliance Process

Step 1: Change Implementation

1. Create feature branch from appropriate base branch
2. Implement changes following coding standards
3. Add comprehensive unit tests for all changes
4. Update documentation as required

Step 2: Review Submission

1. Push changes to remote feature branch
2. Create pull request with detailed description
3. CodeRabbit review automatically triggered
4. Address all CodeRabbit feedback completely

Step 3: Review Completion

1. Ensure all CodeRabbit comments are resolved
2. Verify all automated checks pass
3. Obtain explicit review approval
4. Confirm merge readiness status

Step 4: Merge Authorization

1. Verify complete review approval
2. Confirm all quality gates passed
3. Execute merge with audit trail
4. Validate post-merge functionality

📊 Quality Gates

MANDATORY QUALITY REQUIREMENTS:

Quality Gate	Requirement	Status
CodeRabbit Review	100% Complete	✅ MANDATORY
Unit Test Coverage	100% Python Code	✅ REQUIRED
Documentation Review	All Changes	✅ MANDATORY
Security Review	All Code Changes	✅ REQUIRED
Configuration Review	All Config Changes	✅ MANDATORY

🔄 Review Process Flow

```
Change Implementation
         ↓
Feature Branch Creation
         ↓
Code Development + Testing
         ↓
Pull Request Creation
         ↓
🚨 MANDATORY CodeRabbit Review
         ↓
Review Feedback Resolution
         ↓
Complete Review Approval
         ↓
Quality Gate Validation
         ↓
Merge Authorization
         ↓
Post-Merge Validation
```

📞 Support and Escalation

Review Support:

- CodeRabbit documentation: Configuration Guide (https://docs.coderabbit.ai)
- GitHub App permissions: App Configuration (https://github.com/apps/abacusai/installations/select_target)
- Technical support: Repository maintainers

Policy Escalation:

- Policy violations: Immediate escalation to repository administrators
- Emergency procedures: Requires explicit authorization from repository owners
- Compliance issues: Documented in audit trail with resolution tracking

---

🏆 Policy Benefits

Quality Assurance:

- Consistent code quality across all changes
- Comprehensive security vulnerability detection
- Standardized documentation and formatting
- Reliable testing and validation processes

Risk Mitigation:

- Prevention of defective code deployment
- Early detection of security vulnerabilities
- Consistent compliance with coding standards

- Comprehensive audit trail for all changes

Team Collaboration:

- Standardized review processes
- Knowledge sharing through review feedback
- Consistent quality expectations
- Professional development through code review

🚨 FINAL NOTICE

THIS POLICY IS MANDATORY AND NON-NEGOTIABLE

All contributors must comply with the mandatory review policy. No exceptions will be granted without explicit authorization from repository administrators.

Violation of this policy may result in:
- Immediate reversion of unauthorized changes
- Temporary or permanent access restrictions
- Escalation to organizational leadership
- Formal compliance review procedures

Policy effective: September 22, 2025
Last updated: September 22, 2025
Next review: Quarterly compliance assessment