

Code Review Procedure

Revision: *Initial Release*

Effective: 2026-01-05



1 Purpose

The purpose of this document is to outline the process of reviewing code at Machine Specialties.

Objectives

1. Ensure only high-quality code changes are pushed to production applications
2. Ensure application code following Machine Specialties' coding standards
3. Protect the production environment from malicious code contributions changes
4. Maintain regulatory compliance with CMMC
5. Maintain compliance with Machine Specialties' Change Management policy
6. Maintain compliance with Machine Specialties' Software Development Lifecycle policy

2 Scope

All application code written by Machine Specialties employees or contractors for production applications or information systems.

3 Definitions

SDLC

Software development lifecycle

Static analysis

Checking application code for defects without execution

Dynamic analysis

Checking application functionality during execution

Penetration testing

Testing the application at runtime to identify security weaknesses and vulnerabilities.

4 Process

Before changes are contributed to the main branch of the code repository, the changes must be reviewed and tested for correct functionality, operational security, and data integrity.

4.1 Dependency Management

Software libraries or other types of dependencies such as, but not limited to, CDNs, Container images, Compilers, and Runtime versions, must be audited for security and approved for use in production.

4.2 Review

The following topics must be reviewed

1. Business logic and design
2. Data management
3. Authorization
4. Authentication
5. Session management
6. Exception handling
7. Input validation
8. Logging and auditing
9. Regulatory compliance
10. Documentation

4.3 Documentation

As part of the review process, the code review team verifies that all relevant documentation is created and updated for all changes made. This includes inline code comments, docstrings, public API documentation, user operating manuals, and system administrator manuals.

4.4 Analysis

After the code has been reviewed, it must be proven in a testing environment. The same topics will be tested to verify compliance with Machine Specialties' coding standards and SDLC policy.

4.4.1 Static Analysis

The code review team will use both manual and automated static analysis of application code. Code should be tested to make sure it following industry best practices and meets Machine Specialties' coding standards.

4.4.2 Dynamic Analysis

Dynamic testing should cover the application's behavior, performance, and security. This will verify the application functions in the intended way. This may include testing such as unit testing, integration testing, fuzzing, and performance testing.

4.4.3 Penetration Testing

Applications will be periodically tested using the same techniques as bad actors to determine if there are any security weaknesses or vulnerabilities.

4.5 Release

Once code is reviewed and proven it will be scheduled for release following the Change Management Policy.

5 Enforcement

The code review procedure is enforced by the Director of IT or designated individual.

Noncompliance and violations to this policy will be dealt with according to the sanctions policy.

6 History

Date of Change	Revision	Responsible	Summary of Change
2025-12-16	-	Owen Jacobs	Initial release