

IT Change Control Policy

Revision: *Initial Release*

Effective: 2026-01-05



UNCONTROLLED COPY: ALWAYS VERIFY REVISION

<https://itservices.machspec.com/policies>

1 Purpose

This policy establishes the requirements and processes that the Information Technology Services department uses to identify, document and authorize changes to within the Information Technology environment. It minimizes the likelihood of disruptions, unauthorized alterations and errors.

Objectives

1. Prevent unplanned downtime and system failures.
2. Ensure all changes are documented, tested, and approved.
3. Assign accountability for change implementation.
4. Maintain regulatory compliance with CMMC.

2 Scope

The scope of this process includes, but is not limited to:

- Changes to software developed by Machine Specialties
- All infrastructure hosted in-house or in the cloud
- Information systems and applications that contain company data
- Customer data, regardless of location
- Configuration changes
- Hardware changes
- Process changes

It does not include routine maintenance such as scheduled backups or changes which have an established process signed off by the change authority.

3 Definitions

CAB

Change Advisory Board. The board consists of IT director or manager, system owner, subject matter experts, and key stakeholders identified during the evaluation phase.

Change Authority

The person or group authorizing a change.

CMMC

Cybersecurity Maturity Model Certification

System Owner

The person or group accountable for a system's proper functioning.

4 Policy

This policy requires that all information system changes listed in the scope are formally requested, approved, and adequately communicated to stakeholders.

4.1 Change Control Process

There are, generally, seven stages in our change control process. Planning and evaluation can take place in either order. They are:

1. Planning: Plan the change, including the implementation design, schedule, communication plan, test plan, and roll back plan.
2. Evaluation: Evaluate the change, including determining the risk based in priority level of service and the nature of the proposed change, determining the change type and the change process to use.
3. Review: Review change plan with peers and/or appropriate change authority as determined by the type of change.
4. Communication: Communicate changes with the affected individuals.
5. Implementation: Implement the change according to the approved plan.
6. Documentation: Document the change and any review and approval information.
7. Post-change review: Review the change and note improvements to better achieve our objectives.

4.2 Risk Assessment

During the change assessment we must evaluate the business impact and which systems, services, and users will be affected; the chance of error and potential consequences; any dependencies on the change; and what testing requirements the change will have.

4.2.1 Risk Assessment Instrument

Risk and Change Type Matrix for Normal and Emergency Changes.

- Determine the impact of the change.
- Then assess the urgency of the proposed change (low can generally wait, medium cannot, and high needs to be done ASAP)
- The matrix shows whether the type of change is then a Normal-Low, Medium, or High, or an Emergency Change. Priority is determined according to the Risk Assessment Instrument included below. (Note: A Standard change does not need to use this matrix because risk is controlled by a pre-approved standardized process)

	Low Urgency	Medium Urgency	High Urgency
Organization	Medium	High	<i>Emergency</i>
Department	Medium	High	High
Team	Medium	Medium	High
Individual	Low	Low	Medium

4.3 Approval

The approval process depends on the classification of change. There are three classes of change:

- **Standard:** A repeatable and pre-authorized change which has a documented process and predictable outcome.
- **Normal:** A change that is not an emergency change or a standard change. Normal changes follow the defined steps of the change management process.
- **Emergency:** A change which must be implemented as soon as possible. Must be approved by IT leadership and tested as much as time allows. These changes are not included in a change schedule.

4.4 Review

After a change has been implemented and documented the team will review the following during the next CAB meeting:

- If the plan was executed successfully
- The mean time to restore service functionality
- Incidents / downtime caused by the change
- Feedback from stakeholders
- If a rollback or workaround was needed and executed successfully

5 Enforcement

The change control policy 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
2025-12-26	-	Owen Jacobs	Initial release