Configuration Management Policy

Meridian Precision Components, Inc.

Document ID	POL-CM-001
Version	1.0
Status	Writing sample, not an issued policy
Sample Author	Brian Geis, briangeis.com/samples
Effective Date	2026-09-23
Policy Owner	Director of Operations
Approved By	President
Review Cycle	Annual, or upon significant change to the CUI environment
Classification	Internal Use

Meridian Precision Components, Inc. is a fictitious organization. This document is a writing sample, written to demonstrate policy authorship against NIST SP 800-171 Revision 2, family 3.4, and it has not been issued or assessed.

Contents

1. Purpose....2
2. Scope....2
3. Roles and Responsibilities....3
4. Policy Statement....4
5. Requirements....4
6. Exceptions....7
7. Enforcement....7
8. Related Documents....7
9. Control Traceability....8
10. Definitions....9
11. References....10
12. Revision History....10

1. Purpose

This policy establishes how Meridian Precision Components controls the configuration of information systems that store, process, or transmit Controlled Unclassified Information (CUI).

A system configured correctly at deployment does not remain correct on its own. Software updates change settings, changes made under pressure go unrecorded, and rebuilt systems drift from the configuration that was approved. Without a mechanism to establish what correct means, detect deviation, and govern change, the configuration in place stops matching the configuration in the plan. This policy establishes that mechanism.

This policy addresses NIST SP 800-171 Revision 2, family 3.4, Configuration Management, which DFARS 252.204-7012 and CMMC Level 2 require Meridian to implement.

2. Scope

2.1 Systems in Scope

This policy applies to all systems within the CUI environment, defined as:

- Engineering workstations, meaning the devices on which technical data packages are opened, part programs are prepared, and programs are transferred to the machine tool controllers
- The file server hosting the CUI share
- Backup systems retaining copies of CUI
- Cloud services under contract that store or process CUI
- The domain controller that authenticates users of those systems and applies their configuration policy
- The network infrastructure connecting them

The domain controller is in scope because it provides security functions to the CUI environment rather than merely connecting it, which makes it a Security Protection Asset.

Systems outside the CUI environment are out of scope for this policy's requirements. Two groups are named here because their treatment differs.

The shop floor machine control network is separated from the CUI environment by the network segmentation described in the System Security Plan. Its vendor-supplied controllers nonetheless receive part programs derived from CUI technical data packages, transferred from the engineering workstations under the controls that plan describes and the Media Protection Policy governs, so segmentation alone does not remove them from consideration. Because those controllers can hold CUI-derived data and cannot be fully secured, Meridian treats them as Specialized Assets: recorded in the asset inventory and in the System Security Plan, shown to be managed under Meridian's risk-based practices, and not held to the requirements in Section 5.

The front-office administrative systems are separated by that same segmentation, do not process, store, or transmit CUI, and provide no security protection for the systems that do, so they fall outside the CUI environment entirely. Meridian retains the basis for that determination, and loss of the separation brings those systems into scope.

2.2 Personnel in Scope

This policy applies to all employees, contractors, and third-party service providers who configure, modify, or administer in-scope systems.

2.3 Exclusions

Customer-furnished equipment operated under customer configuration control is excluded, provided the controlling contract documents that arrangement. Exclusions are recorded in the System Security Plan.

2.4 Proportionality

Meridian is a manufacturer with approximately 60 employees and no dedicated information security staff. This policy is written to be performed by the personnel Meridian actually employs.

Where a larger organization would convene a change advisory board, Meridian uses a single documented approval. Where a larger organization would deploy automated configuration monitoring, Meridian uses scheduled manual review against a recorded baseline.

A policy the organization cannot perform is a finding, not a control. Requirements in this document were selected so that they can be executed and evidenced by existing staff. Where a requirement exceeds current capability, it is recorded in the Plan of Action and Milestones rather than asserted here.

3. Roles and Responsibilities

Role	Responsibility
President	Approves this policy and any exception with residual risk rated High
Director of Operations	Owns this policy. Approves changes to baseline configurations. Approves exceptions rated Low or Moderate. Conducts the annual review
IT Administrator	Maintains baseline configurations and the system inventory. Implements approved changes. Performs security impact analysis. Maintains change records. Conducts quarterly baseline verification
Managed Service Provider	Performs configuration work under contract. Submits changes through the process in Section 5.3. Provides evidence of work performed
All Personnel	Do not install software or alter system configuration. Report suspected unauthorized change

Where Meridian's Managed Service Provider performs work described in this policy, Meridian retains accountability. The service contract requires the provider to operate consistently with this policy, and provider performance is reviewed annually.

4. Policy Statement

Meridian establishes, documents, and maintains baseline configurations for all systems in the CUI environment. Changes to those systems are reviewed for security impact, approved before implementation, and recorded. Systems provide only the functionality required for their business purpose. Unauthorized software is prevented from executing, and user-installed software is controlled.

5. Requirements

5.1 Baseline Configurations and System Inventory

Addresses requirement 3.4.1

5.1.1 A baseline configuration shall be documented for each system type in the CUI environment. At minimum, a baseline records the operating system and version, installed software and versions, firmware versions, applied security configuration settings, network configuration, enabled services, and the documentation describing the system.

5.1.2 A system inventory shall be maintained recording, for every device in the CUI environment: asset identifier, device type, physical location, assigned user or function, operating system version, firmware version, the baseline it follows, and a reference to the documentation describing it.

5.1.3 The inventory shall be reviewed and reconciled against physical holdings quarterly. Discrepancies shall be investigated and resolved before the review is closed.

5.1.4 Baselines shall be updated when an approved change alters the configuration they describe. A baseline that no longer reflects deployed systems provides no control value.

5.1.5 Baselines and inventory shall be retained under version control with prior versions preserved, so that the configuration in effect on any past date can be determined.

5.2 Security Configuration Settings

Addresses requirement 3.4.2

5.2.1 Security configuration settings shall be established for each system type and applied before a system enters the CUI environment.

5.2.2 Settings shall be derived from a recognized source, and the source shall be recorded. Acceptable sources include vendor security guidance, the CIS Benchmarks, DISA Security Technical Implementation Guides, and documented internal analysis.

5.2.3 Where a setting from the selected source is not applied, the deviation and the reason shall be recorded. Deviations are expected. Undocumented deviations are not.

5.2.4 For Windows endpoints, Meridian applies a documented hardening baseline maintained under version control, with each setting traceable to its authoritative source and its operational side effects recorded. Application of the baseline captures the prior system state, permitting rollback and providing evidence of the configuration in effect before change.

5.2.5 Engineering workstations and the file server are joined to Meridian's Active Directory domain, and their security configuration settings shall be applied through domain policy. Settings shall be applied locally only where domain policy does not reach the setting, and the mechanism used shall be recorded in the baseline. The machine tool controllers are not domain members and are not configured through domain policy, and their treatment is in Section 2.1. A setting enforced through Group Policy is reasserted at each policy refresh, while a value written directly to the registry is not, and the two carry different verification burdens.

5.2.6 Applied settings shall be verified quarterly against the recorded baseline. Verification results shall be retained as evidence.

5.3 Change Control

Addresses requirements 3.4.3, 3.4.4, and 3.4.5

5.3.1 Changes to systems in the CUI environment, including changes to Group Policy Objects that apply to them, shall be requested in writing before implementation. A request shall identify the system affected, the change proposed, the business reason, and the requester.

5.3.2 The IT Administrator shall perform a security impact analysis before approval, addressing: which security controls the change affects, whether the change introduces new network exposure or access paths, whether it alters the CUI boundary, and how the change is reversed if it fails.

5.3.3 The Director of Operations shall approve or reject each change in writing. Approval records shall identify the approver and the date.

5.3.4 Only the IT Administrator and the Managed Service Provider hold credentials permitting configuration change in the CUI environment, including domain administrative rights. Standard user accounts shall not hold administrative rights on in-scope systems.

5.3.5 Physical access to the servers and network equipment shall be restricted to personnel authorized to make configuration changes.

5.3.6 A change record shall be retained for each implemented change, recording the request, the impact analysis, the approval, the implementation date, who implemented it, and the outcome. Records shall be retained for three years.

5.3.7 **Emergency changes.** A change required to restore service or contain a security incident may be implemented before approval. It shall be recorded and submitted for retroactive review within

two business days. An emergency change that is not subsequently approved shall be reversed or escalated as an exception under Section 6.

5.4 Least Functionality

Addresses requirements 3.4.6 and 3.4.7

5.4.1 Systems shall be configured to provide only the capabilities required for their business purpose.

5.4.2 For each system type, the functions, ports, protocols, and services required shall be documented in the baseline. Anything not documented as required shall be disabled or removed.

5.4.3 Nonessential software present in the vendor image shall be removed during system build.

5.4.4 Remote access services, local administrative shares, legacy authentication protocols, and unused network services shall be disabled unless documented as required.

5.4.5 The list of required functions, ports, protocols, and services shall be reviewed annually. Items no longer required shall be removed and the baseline updated.

5.4.6 Determination of what is essential rests with the Director of Operations in consultation with the IT Administrator. The determination and its reasoning shall be recorded, so that a later reviewer can distinguish a deliberate decision from an oversight.

5.5 Software Execution Control

Addresses requirement 3.4.8

5.5.1 Meridian operates a deny-all, permit-by-exception policy for software execution on engineering workstations, the file server, and the domain controller in the CUI environment.

5.5.2 Execution control shall be implemented through the operating system's native application control capability, configured to permit execution only from directories that standard users cannot write to, plus an explicit list of approved applications.

5.5.3 An authorized software list shall be maintained recording each approved application, its version, its business justification, and the date of approval.

5.5.4 Addition of software to the authorized list follows the change control process in Section 5.3.

5.5.5 **Scope limitation.** Execution control as described applies to engineering workstations, the file server, and the domain controller. It does not apply to the shop floor machine control network, whose vendor-supplied controllers do not support application control. Those assets are treated as Specialized Assets under Section 2.1 and managed under Meridian's risk-based practices, and their treatment is recorded in the System Security Plan.

5.5.6 Before enforcement, execution control shall be operated in audit mode for a period sufficient to identify legitimate software that would otherwise be blocked. Enforcement without this step causes production disruption and predictably results in the control being disabled.

5.6 User-Installed Software

Addresses requirement 3.4.9

5.6.1 Personnel shall not install software on systems in the CUI environment.

5.6.2 Standard users shall not hold the administrative rights required to install software. This restriction is the primary enforcement mechanism. Requirement 5.6.1 states the expectation, and the absence of administrative rights enforces it.

5.6.3 Software required for business purposes shall be requested through the change control process and installed by the IT Administrator.

5.6.4 Installed software shall be reviewed quarterly against the authorized software list. Unauthorized software shall be removed and the occurrence investigated.

6. Exceptions

6.1 Any deviation from this policy requires a documented exception.

6.2 An exception request shall state the requirement not met, the reason, the compensating controls in place, the residual risk, and an expiration date.

6.3 Exceptions with residual risk rated Low or Moderate are approved by the Director of Operations. Exceptions rated High are approved by the President.

6.4 Exceptions shall not exceed twelve months. Continuation requires a new request and fresh risk assessment.

6.5 Open exceptions shall be recorded in the Plan of Action and Milestones and reviewed at each POA&M review.

7. Enforcement

Failure to comply with this policy may result in disciplinary action up to and including termination, and for contractors may result in termination of the contract. Suspected unauthorized configuration change shall be reported to the Director of Operations and handled under the Incident Response Policy.

8. Related Documents

- System Security Plan
- Plan of Action and Milestones
- Access Control Policy (POL-AC-001)
- Incident Response Policy (POL-IR-001)
- Media Protection Policy (POL-MP-001)
- Configuration Management Procedures (PRO-CM-001)

This document states what must be true. Operating instructions, including build steps, verification steps, and the change request form, are maintained in PRO-CM-001.

9. Control Traceability

This matrix maps each requirement in family 3.4 to the policy sections that address it. It is a reading aid rather than a claim of compliance. A security requirement is met when an assessor determines, from evidence, that all applicable assessment objectives are satisfied, and those objectives are stated in NIST SP 800-171A. This policy states what must be true. Section 9.1 names the records that demonstrate it.

NIST SP 800-171A decomposes family 3.4 into 43 lettered assessment objectives and states 3.4.4 as a single determination. This matrix maps at requirement level, because objective-level mapping describes implementation and belongs in the System Security Plan. Two objectives are met by this policy itself: 3.4.8[a], which asks whether a policy specifying the execution control approach exists, and 3.4.9[a], which asks whether a policy for controlling user-installed software is established. Every other objective in the family requires implementation and the evidence Section 9.1 names. Requirement text in this matrix is abbreviated. The authoritative text is in NIST SP 800-171 Revision 2.

800-171 Rev 2	Requirement	Policy Section
3.4.1	Establish and maintain baseline configurations and inventories	5.1.1 through 5.1.5
3.4.2	Establish and enforce security configuration settings	5.2.1 through 5.2.6
3.4.3	Track, review, approve or disapprove, and log changes	5.3.1, 5.3.3, 5.3.6, 5.3.7
3.4.4	Analyze the security impact of changes prior to implementation	5.3.2
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes	5.3.4, 5.3.5
3.4.6	Employ the principle of least functionality	5.4.1, 5.4.2, 5.4.6
3.4.7	Restrict, disable, or prevent use of nonessential programs, functions, ports, protocols, and services	5.4.3, 5.4.4, 5.4.5
3.4.8	Apply a deny-by-exception or deny-all, permit-by-exception policy for software execution	5.5.1 through 5.5.6
3.4.9	Control and monitor user-installed software	5.6.1 through 5.6.4

9.1 Evidence Expected at Assessment

Requirement	Evidence
3.4.1	Baseline documents; system inventory; quarterly reconciliation records
3.4.2	Documented settings with recorded source and applied mechanism; Group Policy Objects for domain-applied settings; deviation register; quarterly verification results
3.4.3	Change records with request, approval, and implementation detail
3.4.4	Security impact analysis within change records
3.4.5	Account listing showing administrative rights; physical access records
3.4.6	Baseline documentation of required functions; annual review record
3.4.7	System configuration showing disabled services; build documentation
3.4.8	Application control configuration; authorized software list; audit mode results
3.4.9	Account listing showing absence of user administrative rights; quarterly software review records

10. Definitions

Baseline configuration. A documented set of specifications for a system, formally reviewed and agreed upon at a given point in time, which serves as the basis for future builds and change, and which is changed only through the change control process.

Controlled Unclassified Information (CUI). Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

CUI environment. The systems, components, and network segments that store, process, or transmit CUI, together with those that provide security protection for them.

Operational Technology. Programmable systems or devices that interact with the physical environment, such as the controllers that operate machine tools.

Out-of-Scope Asset. Under CMMC, an asset that cannot process, store, or transmit CUI and provides no security protection for assets that do. Meridian retains the basis for each such determination.

Security Protection Asset. Under CMMC, an asset that provides security functions or capabilities to the assessed environment. It is assessed against the requirements relevant to what it provides.

Specialized Asset. Under CMMC, an asset that can process, store, or transmit CUI but cannot be fully secured, including Operational Technology and equipment supplied by a customer or the Government. It is documented and managed under risk-based practices rather than held to every requirement.

Least functionality. Configuring a system to provide only the capabilities necessary to accomplish its required function.

Security impact analysis. Evaluation of a proposed change to determine its effect on the security posture of the system.

11. References

- NIST SP 800-171 Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- NIST SP 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*
- 32 CFR Part 170, *Cybersecurity Maturity Model Certification (CMMC) Program*
- 32 CFR Part 2002, *Controlled Unclassified Information (CUI)*

12. Revision History

Version	Date	Change
1.0	2026-09-23	Initial issue