# Plan of Action and Milestones (POA&M)

NIST SP 800-171 Rev 2 - CMMC Level 2 self-assessment

| | |
|---|---|
| **Organization** | Meridian Machining LLC |
| **CAGE code** | 7XYZ1 |
| **Assessment** | Q3 2026 CMMC Level 2 Self-Assessment |
| **Standard** | NIST SP 800-171 Rev 2 (CMMC Level 2) |
| **Assessment scope** | All corporate IT and shop-floor systems processing FCI/CUI at the Manassas, VA facility (12 workstations, 1 file server, ERP, CAD/CAM stations) |
| **POA&M date** | 2026-07-28 |
| **Estimated SPRS score** | 98 of 110 (range -203 to 110, DoD Assessment Methodology v1.2.1) |
| **Conditional status eligible** | Yes (32 CFR 170.21) |
| **Open items** | 12 |

| # | Requirement | Wt | Status | Planned mitigation | Owner | Est. compl. | Milestones |
|---|---|---|---|---|---|---|---|
| 1 | AC.L2-3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after... | 1 | Not implemented | Enforce 10-minute screen lock with pattern-hiding display via Group Policy; verify on shop-floor kiosks. | Office Admin - K. Tran | 2026-09-30 | M1: Pilot on front-office PCs (2026-09-01) |
| 2 | AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and capture the... | 1 | Not implemented | Restrict privileged functions to the two named admin accounts; enable CloudTrail-style audit logging of privileged actions on the file server and ERP. | IT Manager - D. Reyes | 2026-10-31 | M1: Inventory privileged accounts (2026-09-05)<br>M2: Enable privileged-action logging (2026-10-10) |
| 3 | AC.L2-3.1.8 Limit unsuccessful logon attempts | 1 | Not implemented | Enable account lockout after 5 failed logon attempts (30-minute lockout) via Group Policy on the domain. | IT Manager - D. Reyes | 2026-09-30 | M1: GPO change in test OU (2026-09-10) |
| 4 | AC.L2-3.1.9 Provide privacy and security notices consistent with applicable CUI rules | 1 | Not implemented | Deploy DoD-compliant logon banner on all workstations and the VPN portal. | IT Manager - D. Reyes | 2026-09-15 | M1: Banner text legal review (2026-08-25) |
| 5 | AT.L2-3.2.3 Provide security awareness training on recognizing and reporting potential indicators of... | 1 | Not implemented | Add insider-threat indicators module to annual security-awareness training; brief supervisors separately. | President - M. Alvarez | 2026-11-30 | M1: Select training content (2026-10-15) |
| 6 | AU.L2-3.3.3 Review and update logged events | 1 | Not implemented | Quarterly review of audited event types against current threat guidance; document the review in the SSP. | IT Manager - D. Reyes | 2026-11-15 | M1: First quarterly review (2026-10-01) |
| 7 | CM.L2-3.4.4 Analyze the security impact of changes prior to implementation | 1 | Not implemented | Add a security-impact checklist to the change-request form; changes touching CUI systems require sign-off. | IT Manager - D. Reyes | 2026-10-31 | M1: Update change-request form (2026-09-20) |
| 8 | IA.L2-3.5.8 Prohibit password reuse for a specified number of generations | 1 | Not implemented | Enable password-history (24 remembered) in the domain password policy. | IT Manager - D. Reyes | 2026-09-30 | M1: GPO change + verify (2026-09-12) |
| 9 | MA.L2-3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI | 1 | Not implemented | Add sanitization step to the equipment off-site maintenance procedure: drives wiped or removed before shipment. | Shop Foreman - J. Whitfield | 2026-10-15 | M1: Update maintenance SOP (2026-09-15) |

| # | Requirement | Wt | Status | Planned mitigation | Owner | Est. compl. | Milestones |
|---|---|---|---|---|---|---|---|
| 10 | MP.L2-3.8.4 Mark media with necessary CUI markings and distribution limitations.[27] | 1 | Not implemented | Apply CUI markings to backup media and the transfer drives used for customer drawings. | Office Admin - K. Tran | 2026-09-30 | M1: Order CUI labels (2026-08-30) |
| 11 | PE.L2-3.10.4 Maintain audit logs of physical access | 1 | Not implemented | Maintain visitor log at the front desk covering the CNC floor and front office; retain 1 year. | Office Admin - K. Tran | 2026-09-15 | M1: Log book + procedure at front desk (2026-09-01) |
| 12 | RA.L2-3.11.3 Remediate vulnerabilities in accordance with risk assessments | 1 | Not implemented | Remediate scanner findings per severity SLA (critical 30d / high 60d); track in the CyberPolicify risk register. | IT Manager - D. Reyes | 2026-12-15 | M1: Adopt severity SLAs (2026-10-01)<br>M2: Close current criticals (2026-11-15) |

**Affirmation**

This Plan of Action and Milestones reflects the current implementation status of NIST SP 800-171 Rev 2 within the assessment scope stated above, and the planned remediation of all open requirements.

Affirming Official: Maria Alvarez

Title: President

Signature: _____

Date: _____

*Generated by CyberPolicify. Keep this document on file - the SPRS submission itself is the score, date, and scope entered in the PIEE portal by the Affirming Official; the POA&M is provided to prime contractors and assessors on request. Sign in ink or with a digital signature (e.g. Adobe/CAC) as your prime requires.*