datanomix® + Carbide

CMMC 2.0 LEVEL 1 REQUIREMENTS

A checklist for the 15 foundational practices focused on basic cyber hygiene.

CMMC 2.0 Level 1 is the entry point for compliance, focusing on securing Federal Contract Information (FCI). Unlike higher levels, Level 1 allows for self-assessment, which must be completed annually and reported to the **Supplier Performance Risk System** (SPRS). To complete a CMMC 2.0 Level 1 self-assessment, manufacturers must follow 15 practices outlined in **FAR Clause 52.204-21** and ensure they are implemented across all systems.

THE 15 FOUNDATIONAL PRACTICES FOR CMMC 2.0 LEVEL 1 COMPLIANCE

- ☐ **1.** Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- ☐ **2.** Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- ☐ **3.** Verify and control/limit connections to and use of external information systems.
- ☐ **4.** Control information posted or processed on publicly accessible information systems.
- ☐ **5.** Identify information system users, processes acting on behalf of users, or devices.
- ☐ **6.** Authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to information systems.
- ☐ **7.** Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

- [ ] **8.** Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals.

- [ ] **9.** Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

- [ ] **10.** Monitor, control, and protect communications (i.e., information transmitted or received by information systems) at the external boundaries and key internal boundaries of the information systems.

- [ ] **11.** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

- [ ] **12.** Identify, report, and correct information and information system flaws in a timely manner.

- [ ] **13.** Provide protection from malicious code at appropriate locations within information systems.

- [ ] **14.** Update malicious code protection mechanisms when new releases are available.

- [ ] **15.** Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Implementing these controls ensures basic cyber hygiene, providing a foundational layer of security to protect FCI without requiring advanced capabilities. They are the minimal security practices that manufacturers must implement to comply with the requirements of CMMC 2.0 Level 1.

ASSESS YOUR READINESS FOR CMMC 2.0 LEVEL 1 COMPLIANCE

If you're preparing for CMMC 2.0 Level 1 compliance, **Carbide offers a free self-assessment tool** to help you navigate the process. This tool provides step-by-step guidance and generates a report identifying any gaps that need to be addressed to meet the Level 1 requirements.

← SCAN TO ACCESS THE FREE TOOL