www.infoshield.net

To achieve Cybersecurity Maturity Model Certification (CMMC) Level 1 compliance, your organization needs to meet the basic cybersecurity requirements necessary to protect Federal Contract Information (FCI). CMMC Level 1 includes 17 practices focused on safeguarding information at a foundational level. Below is a checklist to help guide your organization toward CMMC Level 1 compliance.

If you'd like additional assistance from InfoShield, contact us through sales@infoshield.net or call 904.310.0897 to schedule a free consultation.

# CMMC Level 1 Compliance Checklist

## Access Control (AC)

AC.1.001 – Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)

AC.1.002 – Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

AC.1.003 – Verify and control and/or limit connections to, and use of, external information systems.

AC.1.004 – Control Information Posted or Processed on Publicly Accessible Information Systems

## Identification and Authentication (IA)

IA.1.076 – Identify Information System Users, Processes Acting on Behalf of Users and Devices

IA.1.077 – Authenticate ( or verify ) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems

## Media Protection (MP)

MP.1.118 – Sanitize or destroy information system media containing Federal contract information before disposal or release for reuse

## Physical Protection (PE)

PE.1.131 – Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

PE.1.132 – Escort Visitors and Monitor Visitor Activity

PE.1.133 – Maintain Audit Logs of Physical Access

PE.1.134 – Control and Manage Physical Access Devices

## System and Communication Protections (SC)

SC.1.175 – Monitor, control, and protect organizational communications (i.e., Information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of information systems.

SC.1.176 – Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks

## System and Information Integrity

SI.1.210 – Identify, Report and Correct Information and Information Flaws in a Timely Manner

SI.1.211 – Provide protection from malicious code at appropriate locations within organizational information systems.

SI.1.212 – Update Malicious Code Protection Mechanisms When New Releases are Available.

SI.1.213 – Perform periodic scans of information systems and real-time scans of files from external sources as files are downloaded, opened or executed.

## References

https://www.acquisition.gov/far/52.204-21