JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

CMMC Level 1 Requirements

The CMMC Level 1 Requirements and Recommendations Table provides detailed information on the assessment objectives for CMMC Level 1 security requirements and a simplified explanation of each objective.

REQUIREMENT I.D.	OBJECTIVE I.D. REQUIREMENT	LEVEL 1 OBJECTIVE I.D.	LEVEL 1 OBJECTIVE	SIMPLE EXPLANATION OF LEVEL 1 OBJECTIVE
AC.L1-b.1.i	Authorized Access Control	AC.L1-b.1.i-[a]	Authorized users are identified	Know who is allowed to use company systems
		AC.L1-b.1.i-[b]	Processes acting on behalf of authorized users are identified	Know what automated programs can access systems
		AC.L1-b.1.i-[c]	Devices (and other systems) authorized to connect to the system are identified	Know which devices can connect to your systems
		AC.L1-b.1.i-[d]	System access is limited to authorized users	Only approved people can log into authorized devices and access the environment
		AC.L1-b.1.i-[e]	System access is limited to processes acting on behalf of authorized users	Only approved applications and service accounts/process can run in environment
		AC.L1-b.1.i-[f]	System access is limited to authorized devices (including other systems)	Only approved computers or devices can connect into the environment
AC.L1-b.1.ii	Transaction & Function Control	AC.L1-b.1.ii-[a]	The types of transactions and functions that authorized users are permitted to execute are defined	Define what each user is allowed to do
		AC.L1-b.1.ii-[b]	System access is limited to the defined types of transactions and functions for authorized users	Make sure systems enforce those limits
AC.L1-b.1.iii	External Connections	AC.L1-b.1.iii-[a]	Connections to external systems are identified	Know what outside systems connect to yours (e.g., do you use Amazon or MS Cloud)
		AC.L1-b.1.iii-[b]	The use of external systems is identified	Approve external systems before connection
		AC.L1-b.1.iii-[c]	Connections to external systems are verified	Limit how those outside connections work
		AC.L1-b.1.iii-[d]	The use of external systems is verified	If connecting to external networks, such as cloud services or other outside organizations, document and approve interconnection

(continued)

REQUIREMENT I.D.	OBJECTIVE I.D. REQUIREMENT	LEVEL 1 OBJECTIVE I.D.	LEVEL 1 OBJECTIVE	SIMPLE EXPLANATION OF LEVEL 1 OBJECTIVE
AC.L1-b.1.iii	External Connections	AC.L1-b.1.iii-[e]	Connections to external systems are controlled/limited	Technically restrict the ability to connect to external systems beyond authorized connections and services
		AC.L1-b.1.iii-[f]	The use of external systems is controlled/limited	Restrict what users, processes and/or devices can connect to authorized external systems/ connections
AC.L1-b.1.iv	Control Public Information	AC.L1-b.1.iv-[a]	Individuals authorized to post or process information on publicly accessible systems are identified	Formally identify the individuals authorized to post or process information on publicly-accessible systems, such as Social Media, the company website, to the media, etc.
		AC.L1-b.1.iv-[b]	Procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified	Have procedures to review information before publicly released
		AC.L1-b.1.iv-[c]	A review process is in place prior to posting of any content to publicly accessible systems	Review public content so sensitive information is not posted
		AC.L1-b.1.iv-[d]	Content on publicly accessible systems is reviewed to ensure that it does not include [FCI]	
		AC.L1-b.1.iv-[e]	Mechanisms are in place to remove and address improper posting of [FCI]	If found be able to remove the information
IA.L1-b.1.v	Identification	IA.L1-b.1.v-[a]	System users are identified	Each user should have a unique identity
		IA.L1-b.1.v-[b]	Processes acting on behalf of users are identified	Have list of service accounts or other accounts that are not actual users
		IA.L1-b.1.v-[c]	Devices accessing the system are identified	Know which devices or processes are authorized to use the system
IA.L1-b.1.vi	Authentication	IA.L1-b.1.vi-[a]	The identity of each user is authenticated or verified as a prerequisite to system access	Users must prove who they are before getting access
		IA.L1-b.1.vi-[b]	The identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access	Systems must actually enforce authentication
		IA.L1-b.1.vi-[c]	The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access	Only allow authorized devices

(continued)

REQUIREMENT I.D.	OBJECTIVE I.D. REQUIREMENT	LEVEL 1 OBJECTIVE I.D.	LEVEL 1 OBJECTIVE	SIMPLE EXPLANATION OF LEVEL 1 OBJECTIVE
MP.L1-b.1.vii	Media Disposal	MP.L1-b.1.vii-[a]	System media containing [FCI] is sanitized or destroyed before disposal	Remove or destroy federal contract information before media is thrown away or reused
		MP.L1-b.1.vii-[b]	System media containing [FCI] is sanitized before it is released for reuse	Have a repeatable process to ensure information is not inadvertently accessed when equipment is reused
PE.L1-b.1.viii	Limit Physical Access	PE.L1-b.1.viii-[a]	Authorized individuals allowed physical access are identified	Know who can physically access your company and resources
		PE.L1-b.1.viii-[b]	Physical access to organizational systems is limited to authorized individuals	Only authorized people can physically reach systems
		PE.L1-b.1.viii-[c]	Physical access to equipment is limited to authorized individuals	Control how people enter those areas
		PE.L1-b.1.viii-[d]	Physical access to operating environments is limited to authorized individuals	Only authorized people can physically reach systems
PE.L1-b.1.ix	Visitor Control	PE.L1-b.1.ix-[a]	Visitors are escorted	Visitors should not move freely in sensitive areas
		PE.L1-b.1.ix-[b]	Visitor activity is monitored	Require authorized individual to escort visitors
		PE.L1-b.1.ix-[c]	Audit logs of physical access are maintained	Keep records of visitor access
		PE.L1-b.1.ix-[d]	Physical access devices are identified	Control and track access tools like keys and badges
		PE.L1-b.1.ix-[e]	Physical access devices are controlled	
		PE.L1-b.1.ix-[f]	Physical access devices are managed	
SC.L1-b.1.x	Boundary Protection	SC.L1-b.1.x-[a]	The external system boundary is defined	Monitor network communications
		SC.L1-b.1.x-[b]	Key internal system boundaries are defined	Protect the points where your network connects to outside networks
		SC.L1-b.1.x-[c]	Communications are monitored at the external system boundary	Log network traffic at firewall
		SC.L1-b.1.x-[d]	Communications are monitored at key internal boundaries	Log network traffic
		SC.L1-b.1.x-[e]	Communications are controlled at the external system boundary	Only allow authorized connections and services
		SC.L1-b.1.x-[f]	Communications are controlled at key internal boundaries	Only allow authorized connections and services
		SC.L1-b.1.x-[g]	Communications are protected at the external system boundary	Use secure communications for sensitive data
		SC.L1-b.1.x-[h]	Communications are protected at key internal boundaries	

(continued)

REQUIREMENT I.D.	OBJECTIVE I.D. REQUIREMENT	LEVEL 1 OBJECTIVE I.D.	LEVEL 1 OBJECTIVE	SIMPLE EXPLANATION OF LEVEL 1 OBJECTIVE
SC.L1-b.1.xi	Public System Separation	SC.L1-b.1.xi-[a]	Publicly accessible system components are identified	Know which systems are accessible to the public
		SC.L1-b.1.xi-[b]	Subnetworks for publicly accessible system components are physically or logically separated from internal networks	Keep public-facing systems separate from internal systems, use technical controls to enforce that separation
SI.L1-b.1.xii	Flaw Remediation	SI.L1-b.1.xii-[a]	The time within which to identify system flaws is specified	How long from when system flaws are known to when those responsible to fix are aware
		SI.L1-b.1.xii-[b]	System flaws are identified within the specified time frame	Review system flaw notifications and identify what applies to your systems
		SI.L1-b.1.xii-[c]	The time within which to report system flaws is specified	When are vulnerability scans conducted?
		SI.L1-b.1.xii-[d]	System flaws are reported within the specified time frame	How are vulnerability scans reviewed/reported?
		SI.L1-b.1.xii-[e]	The time within which to correct system flaws is specified	How long do you allow for patching of systems?
		SI.L1-b.1.xii-[f]	System flaws are corrected within the specified time frame	Ensure patching is conducted within the timeframe specified
SI.L1-b.1.xiii	Malicious Code Protection	SI.L1-b.1.xiii-[a]	Designated locations for malicious code protection are identified	Document where malicious code protection is used
		SI.L1-b.1.xiii-[b]	Protection from malicious code at designated locations is provided	Protect all important places where malware could enter
SI.L1-b.1.xiv	Update Malicious Code Protection	SI.L1-b.1.xiv-[a]	Malicious code protection mechanisms are updated when new releases are available	Keep malware protection tools updated
SI.L1-b.1.xv	System & File Scanning	SI.L1-b.1.xv-[a]	The frequency for malicious code scans is defined	Document when scans will be conducted
		SI.L1-b.1.xv-[b]	Malicious code scans are performed with the defined frequency	Regularly scan systems for malware
		SI.L1-b.1.xv-[c]	Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed	Scan files from outside sources when they are opened or downloaded