#	CMMC Policy	Description
Domain 1: Access Control (AC)		
1	**Limit Information System Access Policy** Authorized Access Control [FCI Data] (AC.L1-b.1.i) *Level: 1*	The purpose of this policy is to ensure information system access is limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2	**Limit System Access to Types of Transaction Policy** Transaction & Function Control [FCI Data] (AC.L1-b.1.ii) *Level: 1*	The purpose of this policy is to ensure information system access is limited to the types of transactions and functions that authorized users are permitted to execute.
3	**Use of External Information Systems Policy** External Connections [FCI Data] (AC.L1-b.1.iii) *Level: 1*	The purpose of this policy is to ensure the organization verifies and controls/limits connections to and use of external information systems.
4	**Publicly Posted Information Policy** Control Public Information [FCI Data] (AC.L1-b.1.iv) *Level: 1*	The purpose of this policy is to ensure the information posted or processed on publicly accessible information systems is controlled.
Domain 5: Identification and Authentication (IA)		
5	**Identification Policy** Identification [FCI Data] (IA.L1-b.1.v) *Level: 1*	The purpose of this policy is to ensure the organization identifies information system users, and processes acting on behalf of users, or devices.
6	**Authenticator Management Policy** Authentication [FCI Data] (IA.L1-b.1.vi) *Level: 1*	The purpose of this policy is to ensure the organization authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Domain 8: Media Protection (MP)		
7	**Sanitize Information System Media Policy** Media Disposal [FCI Data] (MP.L1-b.1.vii) *Level: 1*	The purpose of this policy is to ensure the sanitization or destruction of the information system media containing FCI before disposal or release for reuse is addressed.
Domain 10: Physical Protection (PE)		
8	**Limit Physical Access Policy** Limit Physical Access [FCI Data] (PE.L1-b.1.viii) *Level: 1*	The purpose of this policy is to ensure physical access to organizational information systems, equipment, and the respective operating environments is limited to authorized individuals.

#	CMMC Policy	Description
9	**Manage Visitors and Physical Access Policy** Manage Visitors & Physical Access [FCI Data] (PE.L1-b.1.ix) *Level: 1*	The purpose of this policy is to ensure that visitors are escorted, and their activities are monitored, the organization maintains audit logs of physical access, and the organization controls and manages physical access devices.
Domain 13: System and Communications Protection (SC)		
10	**Boundary Protection Policy** Boundary Protection [FCI Data] (SC.L1-b.1.x) *Level: 1*	The purpose of this policy is to ensure the organization monitors, controls, and protects organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
11	**Implement Subnetworks Policy** Public-Access System Separation [FCI Data] (SC.L1-b.1.xi) *Level: 1*	The purpose of this policy is to ensure the implementation of subnetworks for publicly accessible system components that are physically or logically separated from internal networks is addressed.
Domain 14: System and Information Integrity (SI)		
12	**Flaws Remediation Policy** Flaw Remediation [FCI Data] (SI.L1-b.1.xii) *Level: 1*	The purpose of this policy is to ensure the organization identifies, reports, and corrects information and information system flaws in a timely manner.
13	**Malicious Code Protection Policy** Malicious Code Protection [FCI Data] (SI.L1-b.1.xiii) *Level: 1*	The purpose of this policy is to ensure protection from malicious code is provided at appropriate locations within organizational information systems.
14	**Update Malicious Code Protection Mechanisms Policy** Update Malicious Code Protection [FCI Data] (SI.L1-b.1.xiv) *Level: 1*	The purpose of this policy is to ensure malicious code protection mechanisms are updated when new releases are available.
15	**Malicious Code Scans Policy** System & File Scanning [FCI Data] (SI.L1-b.1.xv) *Level: 1*	The purpose of this policy is to ensure the performance of periodic scans of the information systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
Conflict Resolution Policy		
16	**Conflict Resolution Policy**	The purpose of this policy is to ensure that every employee has the opportunity to raise issues and concerns regarding the workplace environment, interpersonal conflicts, or any

#	CMMC Policy	Description
		misunderstandings, and to have these issues addressed promptly and with respect.