NCP Policy Section	NCP Standard #	NCP Standard Name	Target Audience	Secure Controls Framework (SCF) Control #	CMMC v1.0	NIST 800-171 rev 1	NIST 800-53 rev4	NIST 800-160	ISO 27002 v2013	NIST CSF v1.1
Access Control	AC-01	Account Management	All Users	IAC-15	**AC.1.001** **AC.1.002**	3.1.1 3.1.2	AC-2			PR.AC-1
Access Control	AC-02	Access Enforcement	All Users	IAC-20	**AC.1.001** **AC.1.002**	3.1.1 3.1.2	AC-3		9.2.6 9.4	
Access Control	AC-03	Data Flow Enforcement – Access Control Lists (ACLs)	Technical	NET-04	**AC.2.016**	3.1.3	AC-4		9.4.1 13.11 14.1.2	
Access Control	AC-04	Least Privilege	All Users	IAC-21	**AC.2.007**	3.1.5	AC-6		9.1.2	PR.AC-4
Access Control	AC-05	Authorize Access to Security Functions	Technical	IAC-21.1	**AC.2.007**	3.1.5	AC-6(1)			
Access Control	AC-06	Privileged Accounts	Technical	IAC-21.3	**AC.2.007** **AC.2.008**	3.1.5	AC-6(5)			
Access Control	AC-07	Non-Privileged Access for Non-Security Functions	Technical	IAC-21.2	**AC.2.[illegible]**	3.1.6	AC-6(2)			
Access Control	AC-08	Auditing Use of Privileged Functions	Technical	IAC-21.[illegible]	**AC.3.018**	3.1.7	AC-6(9)			
Access Control	AC-09	Prohibit Non-Privileged Users from Executing Privileged Functions	[illegible]chnical	IAC-21.5	**AC.3.018**	3.1.7	AC-6(10)			
Access Control	AC-10	Account Lockout	All Use[illegible]	IAC-22	**AC.2.009**	3.1.8	AC-7		6.2.1	
Access Control	AC-11	System Use Notification (Logon Banner)	All Users	SEA-18	**AC.2.005**	3.1.9	AC-8			
Access Control	AC-12	Session Lock	All Users	IAC-24	**AC.2.010**	3.1.10	AC-2(5) AC-11			
Access Control	AC-13	Pattern-Hiding Displays	Technical	IAC-24.1	**AC.2.010**	3.1.10	AC-11(1)			
Access Control	AC-14	Session Termination	All Users	IAC-25	**AC.3.019**	3.1.11	AC-12			
Access Control	AC-15	Automated Monitoring & Control	Technical	NET-14.1	**AC.2.013**	3.1.12	AC-17(1)			
Access Control	AC-16	Protection of Confidentiality / Integrity Using Encryption	Technical	NET-14.2	**AC.3.014**	3.1.13	AC-17(2)			

NCP Policy Section	NCP Standard #	NCP Standard Name	Target Audience	Secure Controls Framework (SCF) Control #	CMMC v1.0	NIST 800-171 rev 1	NIST 800-53 rev4	NIST 800-160	ISO 27002 v2013	NIST CSF v1.1
Access Control	AC-17	Managed Access Control Points	Technical	NET-14.3	**AC.2.015**	3.1.14	AC-17(3)			
Access Control	AC-18	Remote Privileged Commands & Sensitive Data Access	Technical	NET-14.4	**AC.3.021**	3.1.15	AC-17(4)			
Access Control	AC-19	Wireless Networking	Technical	NET-15	**AC.2.011**	3.1.16	AC-18			
Access Control	AC-20	Authentication & Encryption	Technical	NET-15.1	**AC.3.012**	3.1.17	AC-18(1)			
Access Control	AC-21	Access Control For Mobile Devices	Technical	MDM-02	**AC.3.020**	3.1.18	AC-19		6.2.1	
Access Control	AC-22	Full Device & Container-Based Encryption	Technical	MDM-03	**AC.3.022**	3.1	AC-19(5)			
Access Control	AC-23	Use of External Information Systems	All Users	DCH-13	**AC.1.0**	3.1.20	AC-20			
Access Control	AC-24	Limits of Authorized Use	Technical	DC	**AC.1.003**	3.1.20	AC-20(1)			
Access Control	AC-25	Portable Storage Devices	Technical	CH-13.2	**AC.2.006**	3.1.21	AC-20(2)			
Access Control	AC-26	Publicly Accessible Content	All Users	DCH-15	**AC.1.004**	3.1.22	AC-22			
Asset Management	AM-01	Asset Governance	All Users	AST-01	**AM.3.036**		PM-5			
Asset Management	AM-02	Security of Assets & Media	All Users	AST-05	**AM.3.036**				11.2.6	
Asset Management	AM-03	Asset Inventories	Management	AST-02	**CM.2.061** **CM.2.064**	3.4.1 3.4.2	CM-8 PM-5		8.1.1	ID.AM-1 ID.AM-2 ID.AM-4
Asset Management	AM-04	Updates During Installations / Removals	Technical	AST-02.1	**CM.2.061** **CM.2.064**	3.4.1 3.4.2	CM-8(1)			
Asset Management	AM-05	Component Duplication Avoidance	Technical	AST-02.3		Non-Federal Organization (NFO)	CM-8(5)			
Audit & Accountability	AU-01	Continuous Monitoring	Technical	MON-01	**AU.2.042** **AU.3.048** **AU.2.044** **AU.3.051** **AU.3.052**	Non-Federal Organization (NFO)	AU-1 SI-4		12.4.1	DE.CM-1 DE.DP-1 DE.DP-2 PR.PT-1

NIST 800-171 rev1 Control #	Requirement Description	Possible Methods To Comply With NIST 800-171 Requirement [administrative actions & commercial tools]	SCF #	Secure Controls Framework (SCF) Control Description
3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users and devices (including other information systems).	- Microsoft Active Directory (AD) - Privileged Account Management (PAM) - Microsoft Active Directory (AD) Network Policy Server (NPS) - Service accounts prohibit interactive login (users cannot log into systems with those accounts).	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, application, guest and temporary accounts.
			IAC-20	Mechanisms exist to enforce logical access permissions through the principle of "least privilege."
			NET-14	Mechanisms exist to define, control and review remote access methods.
3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.		IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, application, guest and temporary accounts.
			IAC-20	Mechanisms exist to enforce logical access permissions through the principle of "least privilege."
			NET-14	Mechanisms exist to define, control and review remote access methods.
3.1.3	Control the flow of sensitive data in accordance with approved authorizations.	- Administrative controls through corporate policies, standards & procedures. - Role-Based Access Controls (RBAC)	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.		HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential malevolent activity without collusion.
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	- Microsoft Active Directory (AD) Group Policy Objects (GPO) - Role-Based Access Controls (RBAC) - Privileged Account Management (PAM)	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.
			IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.
			IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	- Administrative controls through corporate policies, standards & procedures. - Monitoring privileged account usage	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	- Role-Based Access Controls (RBAC)	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.
			IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.
3.1.8	Limit unsuccessful logon attempts.	- Microsoft Active Directory (AD) Group Policy Objects (GPO) - Service/application configuration settings	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.
3.1.9	Provide privacy and security notices consistent with applicable sensitive data rules.	- Logon banner - System use notifications	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides privacy and security notices.
3.1.10	Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.	- Microsoft Active Directory (AD) Group Policy Objects (GPO) - Service/application configuration settings	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user, and retain the session lock until the user reestablishes access using established identification and authentication methods.
			IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.
3.1.11	Terminate (automatically) a user session after a defined condition.		IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.
3.1.12	Monitor and control remote access sessions.	- Security Incident Event Manager (SIEM) - Microsoft Active Directory (AD) Network Policy Server (NPS) - VPN concentrator	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	- Microsoft Active Directory (AD) Network Policy Server (NPS) - VPN concentrator	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions.
3.1.14	Route remote access via managed access control points.		NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	- Administrative controls through corporate policies, standards & procedures. - Monitoring privileged account usage	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.
3.1.16	Authorize wireless access prior to allowing such connections.	- Microsoft Active Directory (AD) Network Policy Server (NPS) - Wireless controller	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.
3.1.17	Protect wireless access using authentication and encryption.		NET-15.1	Authentication and cryptographic mechanisms exist to protect wireless access.
3.1.18	Control connection of mobile devices.	- Mobile Device Management (MDM) solution	MDM-02	Access control mechanisms for mobile devices exist to enforce requirements for the connection of mobile devices to organizational systems.
3.1.19	Encrypt sensitive data on mobile devices.		MDM-03	Cryptographic mechanisms are utilized to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.
3.1.20	Verify and control/limit connections to and use of external information systems.	- Administrative controls through corporate policies, standards & procedures. - Monitoring Internet usage for unauthorized data exfiltration to unauthorized external information systems. - Content filtering by domain/category to block file sharing services.	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.
			DCH-13.1	Mechanisms exist to prohibit external parties, systems and services from storing, processing and transmitting data unless authorized individuals first: ▪ Verifying the implementation of required security controls; or ▪ Retaining a processing agreement with the entity hosting the external systems or service.
3.1.21	Limit use of organizational portable storage devices on external information systems.	- Administrative controls through corporate policies, standards & procedures. - Microsoft Active Directory (AD) Group Policy Objects (GPO)	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.