| # | CMMC Procedure | Description |
|---|---|---|
| **Domain 1: Access Control (AC)** | | |
| 1 | **Limit System Access Procedure**<br>Authorized Access Control [CUI Data] (AC.L2-3.1.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization limits system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). |
| 2 | **Limit System Access to Types of Transaction Procedure**<br>Transaction & Function Control [CUI Data] (AC.L2-3.1.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization limits system access to the types of transactions and functions that authorized users are permitted to execute. |
| 3 | **Control the Flow of CUI Procedure**<br>Control CUI Flow (AC.L2-3.1.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls the flow of CUI according to approved authorizations. |
| 4 | **Separation of Duties Procedure**<br>Separation of Duties (AC.L2-3.1.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization separates the duties of individuals to reduce the risk of malevolent activity without collusion. |
| 5 | **Least Privilege Procedure**<br>Least Privilege (AC.L2-3.1.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization employs the principle of least privilege, including for specific security functions and privileged accounts. |
| 6 | **Non-privilege Accounts or Roles Procedure**<br>Non-Privileged Account Use (AC.L2-3.1.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization uses non-privileged accounts or roles when accessing non-security functions. |
| 7 | **Limit Privilege Functions Procedure**<br>Privileged Functions (AC.L2-3.1.7)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prevents non-privileged users from executing privileged functions and captures the execution of such functions in audit logs. |
| 8 | **Unsuccessful Logins Attempts Procedure**<br>Unsuccessful Logon Attempts (AC.L2-3.1.8)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization limits unsuccessful logon attempts. |
| 9 | **Privacy and Security Notices Procedure**<br>Privacy & Security Notices (AC.L2-3.1.9)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization provides privacy and security notices consistent with applicable CUI rules. |
| 10 | **Session Lock Procedure**<br>Session Lock (AC.L2-3.1.10) | The purpose of this procedure is to ensure the organization uses session locks with pattern-hiding displays to prevent access and viewing |

| # | CMMC Procedure | Description |
|---|---|---|
| | *Level: 2* | of data after a period of inactivity. |
| 11 | **Terminate User Sessions Procedure**<br>Session Termination (AC.L2-3.1.11)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization terminates (automatically) user sessions after a defined condition. |
| 12 | **Remote Access Sessions Procedure**<br>Control Remote Access (AC.L2-3.1.12)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization monitors and controls remote access sessions. |
| 13 | **Encrypt Remote Access Procedure**<br>Remote Access Confidentiality (AC.L2-3.1.13)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization employs cryptographic mechanisms to protect the confidentiality of remote access sessions. |
| 14 | **Use Managed Access Points Procedure**<br>Remote Access Routing (AC.L2-3.1.14)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization routes remote access via managed access control points. |
| 15 | **Authorize Remote Access Procedure**<br>Privileged Remote Access (AC.L2-3.1.15)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization authorizes remote execution of privileged commands and remote access to security-relevant information. |
| 16 | **Authorize Wireless Access Procedure**<br>Wireless Access Authorization (AC.L2-3.1.16)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization authorizes wireless access before allowing such connections. |
| 17 | **Protect Wireless Access Procedure**<br>Wireless Access Protection (AC.L2-3.1.17)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects wireless access using authentication and encryption. |
| 18 | **Control Mobile Connections Procedure**<br>Mobile Device Connection (AC.L2-3.1.18)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls the connection of mobile devices. |
| 19 | **CUI Encryption on Mobile Devices Procedure**<br>Encrypt CUI on Mobile (AC.L2-3.1.19)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization encrypts CUI on mobile devices and mobile computing platforms. |
| 20 | **Use of External Systems Procedure**<br>External Connections [CUI Data] (AC.L2-3.1.20)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization verifies and controls/limits connections to and use of external systems. |

| # | CMMC Procedure | Description |
|---|---|---|
| 21 | **Limit Storage Devices Procedure**<br>Portable Storage Use (AC.L2-3.1.21)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization limits the use of portable storage devices on external systems. |
| 22 | **Publicly Posted Information Procedure**<br>Control Public Information [CUI Data] (AC.L2-3.1.22)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls the CUI posted or processed on publicly accessible systems. |
| 23 | **Asset Control Procedure**<br>Organizationally Controlled Assets (AC.L3-3.1.2e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization restricts access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization. |
| 24 | **Secure Information Transfer Procedure**<br>Secured Information Transfer (AC.L3-3.1.3e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs secure information transfer solutions to control information flows between security domains on connected systems. |
| **Domain 2: Awareness and Training (AT)** | | |
| 25 | **Training Procedure**<br>Role-Based Risk Awareness (AT.L2-3.2.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. |
| 26 | **Role-Based Training Procedure**<br>Role-Based Training (AT.L2-3.2.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure personnel are trained to carry out their assigned information security-related duties and responsibilities. |
| 27 | **Insider Threat Training Procedure**<br>Insider Threat Awareness (AT.L2-3.2.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization provides security awareness training on recognizing and reporting potential indicators of insider threat. |
| 28 | **Advanced Threat Awareness Procedure**<br>Advanced Threat Awareness (AT.L3-3.2.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization provides awareness training upon initial hire, following a significant cyber event, and at least annually, focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat. |
| 29 | **Practical Training Exercise Procedure**<br>Practical Training Exercises (AT.L3-3.2.2e) | The purpose of this procedure is to ensure the organization includes practical exercises in awareness training for all users, tailored by |

| # | CMMC Procedure | Description |
|---|---|---|
| | *Level: 3* | roles to include general users, users with specialized roles, and privileged users, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors. |
| **Domain 3: Audit and Accountability (AU)** | | |
| 30 | **System Audit Logs Procedure**<br>System Auditing (AU.L2-3.3.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization creates and retains system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. |
| 31 | **Unique User Procedure**<br>User Accountability (AU.L2-3.3.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. |
| 32 | **Review Logged Events Procedure**<br>Event Review (AU.L2-3.3.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization reviews, and updates logged events. |
| 33 | **Alert Logging Failure Procedure**<br>Audit Failure Alerting (AU.L2-3.3.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization alerts in the event of an audit logging process failure. |
| 34 | **Correlate Audit Record Procedure**<br>Audit Correlation (AU.L2-3.3.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization correlates audit record review, analysis, and reporting processes for investigation and responds to indications of unlawful, unauthorized, suspicious, or unusual activity. |
| 35 | **Audit Record Reduction Procedure**<br>Reduction & Reporting (AU.L2-3.3.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization provides audit record reduction and report generation to support on-demand analysis and reporting. |
| 36 | **Synchronize System Clocks Procedure**<br>Authoritative Time Source (AU.L2-3.3.7)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization provides a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. |
| 37 | **Audit Logging Tools Procedure**<br>Audit Protection (AU.L2-3.3.8)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects audit information and audit logging tools from unauthorized access, modification, and deletion. |
| 38 | **Audit Logging Functionality Procedure**<br>Audit Management (AU.L2-3.3.9) | The purpose of this procedure is to ensure the organization limits the management of audit logging functionality to a subset of privileged |

| # | CMMC Procedure | Description |
|---|---|---|
| | *Level: 2* | users. |
| **Domain 4: Configuration Management (CM)** | | |
| 39 | **Baseline Configuration Procedure**<br>System Baselining (CM.L2-3.4.1)<br>*Level: 2* | The purpose of this procedure is to ensure the organization establishes and maintains baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. |
| 40 | **Configuration Settings Procedure**<br>Security Configuration Enforcement (CM.L2-3.4.2)<br>*Level: 2* | The purpose of this procedure is to ensure the organization establishes and enforces security configuration settings for information technology products employed in organizational systems. |
| 41 | **Configuration Change Control Procedure**<br>System Change Management (CM.L2-3.4.3)<br>*Level: 2* | The purpose of this procedure is to ensure the organization tracks, reviews, approves, or disapproves, and log changes to organizational systems. |
| 42 | **Security Impact Analyses Procedure**<br>Security Impact Analysis (CM.L2-3.4.4)<br>*Level: 2* | The purpose of this procedure is to ensure the organization analyzes the security impact of changes prior to implementation. |
| 43 | **Access Restriction Change Procedure**<br>Access Restrictions for Change (CM.L2-3.4.5)<br>*Level: 2* | The purpose of this procedure is to ensure the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to organizational systems. |
| 44 | **Least Functionality Procedure**<br>Least Functionality (CM.L2-3.4.6)<br>*Level: 2* | The purpose of this procedure is to ensure the organization employs the principle of least functionality by configuring organizational systems to provide only essential capabilities. |
| 45 | **Prevent Nonessential Services Procedure**<br>Nonessential Functionality (CM.L2-3.4.7)<br>*Level: 2* | The purpose of this procedure is to ensure the organization restricts, disables, or prevents the use of nonessential programs, functions, ports, protocols, and services. |
| 46 | **Blacklisting and Whitelisting Software Procedure**<br>Application Execution Policy (CM.L2-3.4.8)<br>*Level: 2* | The purpose of this procedure addresses deny-by-exception (blacklisting) policy to ensure the organization prevents the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. |
| 47 | **User-installed Software Procedure**<br>User-Installed Software (CM.L2-3.4.9)<br>*Level: 2* | The purpose of this procedure is to ensure the organization controls and monitors user-installed software. |

| # | CMMC Procedure | Description |
|---|---|---|
| 48 | **Authoritative Repository Procedure**<br>Authoritative Repository (CM.L3-3.4.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization establishes and maintains an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components. |
| 49 | **Automated Detection and Remediation Procedure**<br>Automated Detection & Remediation (CM.L3-3.4.2e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place the components in a quarantine or remediation network to facilitate patching, re-configuration, or other mitigations. |
| 50 | **Automated Inventory Procedure**<br>Automated Inventory (CM.L3-3.4.3e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. |
| **Domain 5: Identification and Authentication (IA)** | | |
| 51 | **Identification Procedure**<br>Identification [CUI Data] (IA.L2-3.5.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization identifies system users, processes acting on behalf of users, and devices. |
| 52 | **Authenticator Management Procedure**<br>Authentication [CUI Data] (IA.L2-3.5.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems. |
| 53 | **Multifactor Authentication Procedure**<br>Multifactor Authentication (IA.L2-3.5.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization uses multifactor authentication for local and network access to privileged accounts and network access to non-privileged accounts. |
| 54 | **Replay-Resistant Procedure**<br>Replay-Resistant Authentication (IA.L2-3.5.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization employs replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. |
| 55 | **Prevent Reuse of System Identifiers Procedure**<br>Identifier Reuse (IA.L2-3.5.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prevents the reuse of identifiers for a defined period. |
| 56 | **Disable Inactive Accounts Procedure**<br>Identifier Handling (IA.L2-3.5.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization disables identifiers after a defined period of inactivity. |

| # | CMMC Procedure | Description |
|---|---|---|
| 57 | **Password Complexity Procedure**<br>Password Complexity (IA.L2-3.5.7)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization enforces minimum password complexity and change of characters when new passwords are created. |
| 58 | **Prohibition of Password Reuse Procedure**<br>Password Reuse (IA.L2-3.5.8)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prohibits password reuse for a specified number of generations. |
| 59 | **Temporary Password Procedure**<br>Temporary Passwords (IA.L2-3.5.9)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization addresses temporary password use for system logons with an immediate change to a permanent password. |
| 60 | **Cryptographic Password Procedure**<br>Cryptographically-Protected (IA.L2-3.5.10)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization stores and transmits only cryptographically protected passwords. |
| 61 | **Authenticator Feedback Procedure**<br>Obscure Feedback (IA.L2-3.5.11)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization obscures feedback of authentication information. |
| 62 | **Bidirectional Authentication Procedure**<br>Bidirectional Authentication (IA.L3-3.5.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization identifies and authenticates systems and system components, where possible, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant. |
| 63 | **Untrusted Asset Blocking Procedure**<br>Block Untrusted Assets (IA.L3-3.5.3e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile. |
| **Domain 6: Incident Response (IR)** | | |
| 64 | **Incident Handling Capability Procedure**<br>Identifier Handling (IR.L2-3.6.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization establishes an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. |
| 65 | **Incident Reporting Procedure**<br>Incident Reporting (IR.L2-3.6.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization tracks, documents, and reports incidents to designated officials and/or authorities both internal and external to the organization. |

| # | CMMC Procedure | Description |
|---|---|---|
| 66 | **Incident Response Testing Procedure**<br>Incident Reporting Testing (IR.L2-3.6.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization tests the organizational incident response capability. |
| 67 | **Security Operations Center Capability Procedure**<br>Security Operations Center (IR.L3-3.6.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization establishes and maintains a security operations center capability that operates 24/7, with allowance for remote/on-call staff. |
| 68 | **Cyber Incident Response Team Deployment Procedure**<br>Cyber Incident Response Team (IR.L3-3.6.2e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization establishes and maintains a cyber incident response team that can be deployed by the organization within 24 hours. |
| **Domain 7: Maintenance (MA)** | | |
| 69 | **System Maintenance Procedure**<br>Perform Maintenance (MA.L2-3.7.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization performs maintenance on organizational systems. |
| 70 | **System Maintenance Tools Procedure**<br>System Maintenance Control (MA.L2-3.7.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization provides controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. |
| 71 | **Sanitize Equipment Removed Off-site Procedure**<br>Equipment Sanitization (MA.L2-3.7.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization ensures equipment removed for off-site maintenance is sanitized of any CUI. |
| 72 | **Check Maintenance Media for Malicious Code Procedure**<br>Media Inspection (MA.L2-3.7.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization checks media containing diagnostic and test programs for malicious code before the media are used in organizational systems. |
| 73 | **Nonlocal Maintenance Procedure**<br>Nonlocal Maintenance (MA.L2-3.7.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization addresses multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminates such connections when nonlocal maintenance is complete. |
| 74 | **Supervise Maintenance Activities Procedure**<br>Maintenance Personnel (MA.L2-3.7.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization supervises the maintenance activities of personnel without required access authorization. |

| # | CMMC Procedure | Description |
|---|---|---|
| **Domain 8: Media Protection (MP)** | | |
| 75 | **Protect System Media Containing CUI Procedure**<br>Media Protection (MP.L2-3.8.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects (i.e., physically control and securely store) system media containing CUI, both paper and digital. |
| 76 | **Limit Access to CUI on System Media Procedure**<br>Media Access (MP.L2-3.8.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization limits access to CUI on system media to authorized users. |
| 77 | **Sanitize System Media Procedure**<br>Media Disposal [CUI Data] (MP.L2-3.8.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization addresses sanitization or destruction of the system media containing CUI before disposal or release for reuse. |
| 78 | **CUI Markings Procedure**<br>Media Markings (MP.L2-3.8.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization marks media with necessary CUI markings and distribution limitations. |
| 79 | **Control Access to Media Procedure**<br>Media Accountability (MP.L2-3.8.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls access to media containing CUI and maintains accountability for media during transport outside of controlled areas. |
| 80 | **Encrypt CUI on Digital Media Procedure**<br>Portable Storage Encryption (MP.L2-3.8.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization addresses the implementation of cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. |
| 81 | **Control Use of Removable Media Procedure**<br>Removable Media (MP.L2-3.8.7)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls the use of removable media on system components. |
| 82 | **Prohibit Portable Storage Devices Procedure**<br>Shared Media (MP.L2-3.8.8)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prohibits the use of portable storage devices when such devices have no identifiable owner. |
| 83 | **Protect CUI at Storage Locations Procedure**<br>Protect Backups (MP.L2-3.8.9)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects the confidentiality of backup CUI at storage location. |

| # | CMMC Procedure | Description |
|---|---|---|
| **Domain 9: Personnel Security (PS)** | | |
| 84 | **Screening Individuals Procedure**<br>Screen individuals (PS.L2-3.9.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization screens individuals prior to authorizing access to organizational systems containing CUI. |
| 85 | **Personnel Termination and Transfers Procedure**<br>Personnel Actions (PS.L2-3.9.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization ensures organizational systems containing CUI are protected during and after personnel actions, such as terminations and transfers. |
| 86 | **Adverse Information Management and CUI Access Procedure**<br>Adverse Information (PS.L3-3.9.2e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI. |
| **Domain 10: Physical Protection (PE)** | | |
| 87 | **Limit Physical Access Procedure**<br>Limit Physical Access [CUI Data] (PE.L2-3.10.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization limits physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. |
| 88 | **Monitoring Physical Access Procedure**<br>Monitor Facility (PE.L2-3.10.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects and monitors the physical facility and supports infrastructure for organizational systems. |
| 89 | **Escort and Monitor Visitors Procedure**<br>Escort Visitors [CUI Data] (PE.L2-3.10.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization escorts visitors and monitors visitor activity. |
| 90 | **Maintain Physical Access Log Procedure**<br>Physical Access Logs [CUI Data] (PE.L2-3.10.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization maintains audit logs of physical access. |
| 91 | **Control Physical Access Procedure**<br>Manage Physical Access [CUI Data] (PE.L2-3.10.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls and manages physical access devices. |
| 92 | **Protect CUI at Alternate Work Sites Procedure**<br>Alternative Work Sites (PE.L2-3.10.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization enforces safeguarding measures for CUI at alternate work sites. |

| # | CMMC Procedure | Description |
|---|---|---|
| **Domain 11: Risk Assessment (RA)** | | |
| 93 | **Periodically Assess Risk Procedure**<br>Risk Assessments (RA.L2-3.11.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization periodically assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. |
| 94 | **Systems Vulnerability Scans Procedure**<br>Vulnerability Scan (RA.L2-3.11.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization scans for vulnerabilities in organizational systems and applications periodically, and when new vulnerabilities affecting those systems and applications are identified. |
| 95 | **Remediate Vulnerabilities Procedure**<br>Vulnerability Remediation (RA.L2-3.11.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization remediates vulnerabilities in accordance with risk assessments. |
| 96 | **Threat-Informed Risk Assessment Procedure**<br>Threat-Informed Risk Assessment (RA.L3-3.11.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs threat intelligence, at a minimum from open or commercial sources, and any DoD provided sources, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities. |
| 97 | **Threat Hunting Procedure**<br>Threat Hunting (RA.L3-3.11.2e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization conducts cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls. |
| 98 | **Advanced Risk Identification Procedure**<br>Advanced Risk Identification (RA.L3-3.11.3e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components. |
| 99 | **Security Solution Rationale Procedure**<br>Security Solution Rationale (RA.L3-3.11.4e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization documents or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination. |
| 100 | **Security Solution Effectiveness Procedure**<br>Security Solution Effectiveness | The purpose of this procedure is to ensure the organization assess the effectiveness of |

| # | CMMC Procedure | Description |
|---|---|---|
| | (RA.L3-3.11.5e)<br><br>*Level: 3* | security solutions at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence. |
| 101 | **Supply Chain Risk Response Procedure**<br>Supply Chain Risk Response (RA.L3-3.11.6e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization assess, respond to, and monitor supply chain risks associated with organizational systems and system components. |
| 102 | **Supply Chain Risk Procedure**<br>Supply Chain Risk Plan (RA.L3-3.11.7e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization develops a plan for managing supply chain risks associated with organizational systems and system components; update the plan at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident. |
| **Domain 12: Security Assessment (CA)** | | |
| 103 | **Periodically Assess Effectiveness of Security Controls Procedure**<br>Security Control Assessment (CA.L2-3.12.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization periodically assesses the security controls in organizational systems to determine if the controls are effective in their application. |
| 104 | **Operational Plans of Action Procedure**<br>Operational Plan of Action (CA.L2-3.12.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization develops and implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. |
| 105 | **Monitor Security Controls Procedure**<br>Security Control Monitoring (CA.L2-3.12.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization monitors security controls on an ongoing basis to ensure the continued effectiveness of the controls. |
| 106 | **System Security Plans Procedure**<br>System Security Plans (CA.L2-3.12.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization develops, documents, and periodically updates system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. |
| 107 | **Penetration Testing Procedure**<br>Penetration Testing (CA.L3-3.12.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization conducts penetration testing at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests |

| # | CMMC Procedure | Description |
|---|---|---|
| | | using subject matter experts. |
| **Domain 13 System and Communications Protection (SC)** | | |
| 108 | **Boundary Protection Procedure**<br>Boundary Protection [CUI Data] (SC.L2-3.13.1)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization monitors, controls, and protects communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of the organizational systems. |
| 109 | **Systems Security Engineering Principles Procedure**<br>Security Engineering (SC.L2-3.13.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization employs architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. |
| 110 | **Separate User Functionality Procedure**<br>Role Separation (SC.L2-3.13.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization separates user functionality from system management functionality. |
| 111 | **Shared System Resources Procedure**<br>Shared Resource Control (SC.L2-3.13.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prevents unauthorized and unintended information transfer via shared system resources. |
| 112 | **Implement Subnetworks Procedure**<br>Public-Access System Separation [CUI Data] (SC.L2-3.13.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization addresses the implementation of subnetworks for publicly accessible system components that are physically or logically separated from internal networks. |
| 113 | **Deny Network Communications Procedure**<br>Network Communication by Exception (SC.L2-3.13.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). |
| 114 | **Prevent Split Tunneling Procedure**<br>Split Tunneling (SC.L2-3.13.7)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prevents remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). |
| 115 | **Implement Cryptographic Mechanisms Procedure**<br>Data in Transit (SC.L2-3.13.8)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. |

| # | CMMC Procedure | Description |
|---|---|---|
| 116 | **Terminate Network Sessions Procedure**<br>Connections Termination (SC.L2-3.13.9)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. |
| 117 | **Cryptographic Keys Procedure**<br>Key Management (SC.L2-3.13.10)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization establishes and manages cryptographic keys for cryptography employed in organizational systems. |
| 118 | **FIPS-Validated Cryptography Procedure**<br>CUI Encryption (SC.L2-3.13.11)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization employs FIPS-validated cryptography when used to protect the confidentiality of CUI. |
| 119 | **Collaborative Computing Devices Procedure**<br>Collaborative Device Control (SC.L2-3.13.12)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization prohibits remote activation of collaborative computing devices and provides indication of devices in use to users present at the device. |
| 120 | **Mobile Code Procedure**<br>Mobile Code (SC.L2-3.13.13)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls and monitors the use of mobile code. |
| 121 | **VOIP Technologies Procedure**<br>Voice over Internet Protocol (SC.L2-3.13.14)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization controls and monitors the use of Voice over Internet Protocol (VoIP) technologies. |
| 122 | **Sessions Authenticity Procedure**<br>Communications Authenticity (SC.L2-3.13.15)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects the authenticity of communications sessions. |
| 123 | **Protect CUI at Rest Procedure**<br>Data at Rest (SC.L2-3.13.16)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization protects the confidentiality of CUI at rest. |
| 124 | **Physical and Logical Isolation Techniques Procedure**<br>Isolation (SC.L3-3.13.4e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization employs physical isolation techniques or logical isolation techniques or both in organizational systems and system components. |
| **Domain 14: System and Information Integrity (SI)** | | |
| 125 | **Flaws Remediation Procedure**<br>Flaw Remediation [CUI Data] (SI.L2-3.14.1) | The purpose of this procedure is to ensure the organization identifies, reports, and corrects system flaws in a timely manner. |

| # | CMMC Procedure | Description |
|---|---|---|
| | *Level: 2* | |
| 126 | **Malicious Code Protection Procedure**<br>Malicious Code Protection [CUI Data] (SI.L2-3.14.2)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization provides protection from malicious code at appropriate locations within organizational systems. |
| 127 | **Monitor Security Alerts Procedure**<br>Security Alerts & Advisories (SI.L2-3.14.3)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization monitors system security alerts and advisories and takes action in response. |
| 128 | **Update Malicious Code Protection Mechanisms Procedure**<br>Update Malicious Code Protection [CUI Data] (SI.L2-3.14.4)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization updates malicious code protection mechanisms when new releases are available. |
| 129 | **Malicious Code Scans Procedure**<br>System & File Scanning [CUI Data] (SI.L2-3.14.5)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization addresses the performance of periodic scans of the organizational system and real-time scans of files from external sources as files are downloaded, opened, or executed. |
| 130 | **System Monitoring Procedure**<br>Monitor Communications for Attacks (SI.L2-3.14.6)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization monitors organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. |
| 131 | **Identify Unauthorized Use Procedure**<br>Identify Unauthorized Use (SI.L2-3.14.7)<br><br>*Level: 2* | The purpose of this procedure is to ensure the organization identifies unauthorized use of organizational systems. |
| 132 | **Software Integrity Verification Procedure**<br>Integrity Verification (SI.L3-3.14.1e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization verifies the integrity of security critical and essential software using root of trust mechanisms or cryptographic signatures. |
| 133 | **Specialized Assets Security Procedure**<br>Specialized Asset Security (SI.L3-3.14.3e)<br><br>*Level: 3* | The purpose of this procedure is to ensure that specialized assets, including IoT, IIoT, OT, GFE, restricted information systems, and test equipment, are included in the scope of specified enhanced security requirements or are segregated into purpose-specific networks. |

| # | CMMC Procedure | Description |
|---|---|---|
| 134 | **Threat Indicator Utilization and Mitigation Procedure**<br>Threat-Guided Intrusion Detection (SI.L3-3.14.6e)<br><br>*Level: 3* | The purpose of this procedure is to ensure the organization uses threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources and any DoD-provided sources to guide and inform intrusion detection and threat hunting. |
| **Conflict Resolution Procedure** | | |
| 135 | **Conflict Resolution Procedure** | The purpose is to ensure that every employee has the opportunity to raise issues and concerns regarding the workplace environment, interpersonal conflicts, or any misunderstandings, and to have these issues addressed promptly and with respect. |