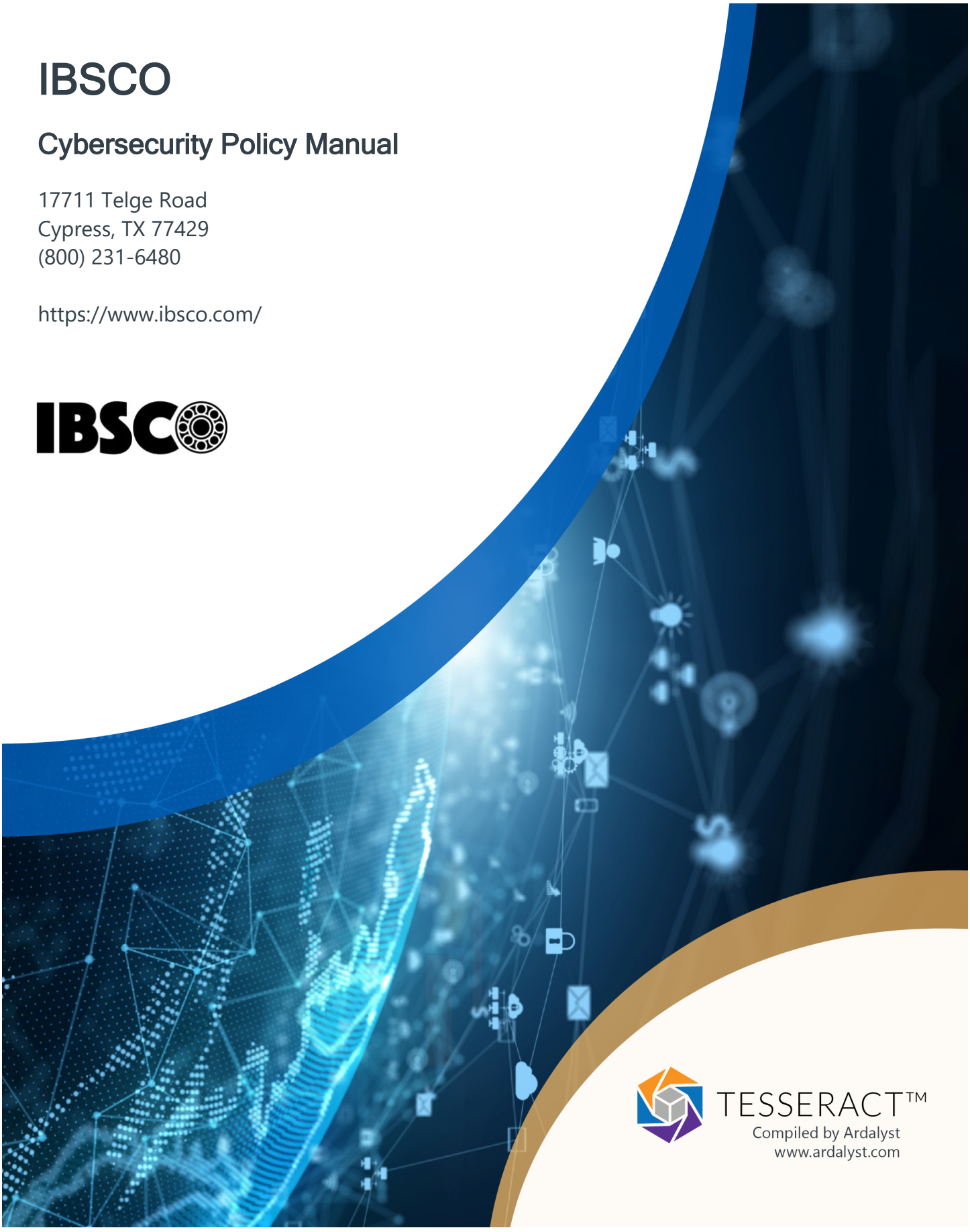
IBSCO

Cybersecurity Policy Manual

17711 Telge Road
Cypress, TX 77429
(800) 231-6480

https://www.ibsco.com/



TESSERACT™
Compiled by Ardalyst
www.ardalyst.com

Disclaimers and Disclosures

This document is developed based on information provided by the Organization Seeking Certification (OSC) ("you", "your") regarding the classification and flow of CUI in your organization and the systems you use (or will use) in your end-state configuration. Their accuracy is dependent on the information you provided. The responsibility for identifying and designating CUI rests solely on you. Nothing in this document should be construed as legal advice. Ardalyst does not determine, interpret, or classify what constitutes Controlled Unclassified Information (CUI) or derivative CUI within your environment. For any determinations regarding CUI, derivative CUI, or related regulatory interpretations, you should consult qualified legal counsel.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Cybersecurity Policy Manual (CPM) Approval

The policies contained herein are approved for immediate implementation and are authorized until replaced. This Cybersecurity Program is governed by DFARS 252.204-7012, 252.204-7019, 252.204-7020, and 252.204-7021, including the guidance provided in NIST SP 800-171, the Cybersecurity Maturity Model Level 2 Certification, the Cybersecurity Maturity Model Level 2 Scoping Guide, and the Cybersecurity Maturity Model Certification Level 2 Assessment Guides. Additional guidelines, if relevant, are noted in each policy.

Signed:

Richard Scroggins

Signature

Richard Scroggins

Printed Name

Technology Manager

Title

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Revision History

This document is updated annually at a minimum.

Version Number	Date Last Completed	Notes	Date Next Due
1.0	2024-05-30	Initial Document	2025-05-30
2.0	2026-01-28	Annual Update	2027-01-28
3.0	2026-08-27	Program Update	2027-08-27

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.1 Access Control Policy

The purpose of the Access Control Policy is to set the standards by which users are allowed to access the organization's networks. These standards improve the security of the organization's networks by limiting access to resources and applying the principle of least privilege to increase the difficulty of malicious activity by an insider. The policy also communicates requirements for acceptable use at login to ensure those connecting understand their obligations when using the system.

Authorized Access Control Section

AC.L2-3.1.1

System access must be strictly limited to authorized users, processes acting on behalf of authorized users, and authorized devices. Unauthorized users, processes, or devices must be denied access by default. System access includes both internal and external systems that are permitted to connect to the enclave. Access control policies must be enforced through mechanisms such as role-based access, cryptographic methods, and identity-based policies.

Authorized users and their roles, service principals and systems authorized to connect must be documented in the User, Process, and Asset Inventory. This documentation must include: a unique identifier for each item tracked within the organization; first and last name of personnel; user principal name (UPN) of user accounts; and a device identifier for devices. Authentication methods for each system must be detailed in the System Security Plan (SSP), ensuring traceability and accountability for all access events. These measures control access between active entities (users or processes) and passive entities (devices, files, records).

The enrollment of users, service principals, and assets into the enclave must follow controls to maintain the integrity of the access control environment. User access must be explicitly approved. User identifiers must be registered in the authentication system before any connection is permitted. Service principals must be approved and added to the authentication system prior to use. These automated identities must be treated with the same rigor as human users, including auditability and access restrictions. All assets must be logged and monitored.

Transactions and Functions Control Section

AC.L2-3.1.2

There are two types of authorized users. These types are standard users and privileged users.

Standard users are permitted to execute the transactions and functions listed in the System Catalog on a per-system basis. Privileged users are permitted to execute the same default user transactions and functions as standard users, but they are also given additional transactions and functions as a result of the assignment of privileged access. Privileged functions are identified in the System Catalog and privileged function assignment is recorded in the User, Process, and Asset Inventory. Privileged users are restricted from accessing productivity transactions and functions.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

CUI Flow Section

AC.L2-3.1.3

The flow of Controlled Unclassified Information (CUI) must be clearly defined, actively controlled, and consistently enforced to ensure its confidentiality, integrity, and compliance with federal requirements. A CUI Flow Diagram must be created to map how CUI is received, handled, and transmitted within the environment. Collaborating with system owners, security personnel, and data custodians during the development of the CUI Flow Diagram helps ensure it accurately reflects the actual system architecture, including all relevant systems, users, and data pathways. This document is essential for understanding where CUI resides, how it moves, and how it is protected.

The CUI Flow Diagram must illustrate the full lifecycle of CUI: how it is received, stored, processed, transmitted, and disposed or shared. Each stage must be clearly documented. It must identify all systems, components, and users involved in handling CUI, including internal systems, external connections, boundary protections, and third-party services. The document must describe the methods and enforcement mechanisms used to control CUI flow. These controls must be explained in terms of how they are applied and how they prevent unauthorized access or transmission. The CUI Flow Diagram must be updated if any of these things significantly change.

Separation of Duties Section

AC.L2-3.1.4

Organizations must establish logical separation of duties through access restrictions to prevent unauthorized configuration changes, malevolent activity, and the misuse of privileges. Separation of duties must be required for audit-related functions including the configuration, management, and review of audit logs and audit logging tools. Roles must be defined in the User, Process, and Asset Inventory and assigned the least amount of privilege necessary to perform required responsibilities. Role-Based Access Control (RBAC) must be used to enforce these role definitions and ensure that users only have access to the functions necessary for their job duties. Non-privileged users and roles, also defined in the User, Process, and Asset Inventory, must not be permitted to perform privileged commands or access sensitive system functions. This separation ensures that no single user has unchecked control over critical system functions, reducing the risk of errors or intentional misuse.

Privileged users are those who have more permissive access than standard users, including access to sensitive information, system configuration settings, and the ability to modify documents pertaining to the program. The list of privileged users must be tightly controlled, with editing rights restricted to a small number of trusted personnel. While it is acceptable for other members of the organization to view the list, editing privileges must be limited to prevent unauthorized changes. The organization must track privileged personnel, their accounts across systems, and the specific levels of access associated with each account. Maintaining a dedicated and controlled list of privileged accounts helps ensure transparency, accountability, and proper oversight of elevated access.

The execution of privileged functions must be captured in audit logs to support accountability and enable incident response. These audit logs must be alerted on for suspicious activity, and these alerts must be reviewed regularly.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Least Privilege Section

AC.L2-3.1.5

When determining the level of access a privileged account should have, the principle of least privilege must be applied. Privileged users must only be assigned the minimum level of access necessary to complete their job duties, and nothing more. Access to privileged accounts must be authorized in accordance with the principle of least privilege. This approach helps reduce the potential for misuse of elevated privileges and limits the impact of compromised accounts.

Roles used to perform changes to configurations or systems must be assigned only to authorized personnel who possess the requisite skill set and training. All changes made by privileged roles must be authorized, documented, logged, and monitored in accordance with the Configuration Management Policy. Privileged accounts must be identified and documented in the User, Process, and Asset Inventory.

Privileged accounts must follow the naming convention a_firstname.lastname to be granted appropriate access according to their role. All admin accounts are prefixed with “a_” to indicate their status as privileged accounts. Privileged accounts must not have email access, either by not assigning a license or by explicitly disabling email functionality to reduce exposure to phishing and other email-based threats. Exceptions may be made for privileged accounts involved in billing, but their access must be limited strictly to billing-related functions.

Non-Privileged Account Use Section

AC.L2-3.1.6

Non-security functions are defined as any function that does not require privileged access. Privileged accounts must not be used to perform non-security or non-privileged tasks. Users with both privileged and non-privileged roles must use separate accounts for each function. Systems must be configured to enforce this separation by restricting access to non-privileged functions from privileged accounts. Administrators must be trained to understand and adhere to this policy, ensuring that privileged credentials are only used for authorized administrative functions.

Non-privileged accounts must follow a standardized naming convention of "firstname.lastname" and must not be assigned privileged access. Privileged accounts must follow a standard naming convention of "a_firstname.lastname" and must not have access to non-security functions, such as productivity tools. This naming convention supports traceability and simplifies account management while reinforcing the separation between standard user and administrative access.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Privileged Functions Section

AC.L2-3.1.7

Privileged functions are operations that require elevated permissions to manage or configure a system. These functions include administrative tasks such as user management, system configuration, and changes to access controls. Accounts that are granted access to perform these functions are referred to as privileged accounts.

Privileged accounts must be uniquely identifiable and consistently labeled. In this environment, privileged accounts are designated by an "a_" prefix in the username. This naming convention supports clear identification and simplifies access control and auditing processes. Non-privileged accounts are defined as those without access to privileged functions. These accounts follow the standard username format and do not include the "a_" prefix. This distinction ensures that access rights are clearly separated and consistently enforced.

Privileged functions are identified in the System Catalog and privileged function assignments are documented in the User, Process, and Asset Inventory.

Systems must be configured to prevent non-privileged accounts from executing privileged functions. This includes enforcing role-based access controls and applying the principle of least privilege to limit access to only what is necessary for each user's role. These controls help prevent unauthorized changes, reduce the risk of misconfiguration, and protect against insider threats.

Systems must also be configured to capture the execution of privileged functions in audit logs, which allows monitoring of their use and aids in detection of unauthorized privileged access.

Unsuccessful Logon Attempts Section

AC.L2-3.1.8

The means of limiting unsuccessful logon attempts is defined in the System Baseline Standard.

The number of unsuccessful logon attempts is defined as no more than ten (10) attempts.

If this threshold is exceeded, the user account must be automatically locked. This lockout mechanism is implemented to mitigate brute-force attacks by introducing a delay that discourages repeated credential guessing. To ensure consistent enforcement, the lockout policy must apply to all user accounts and access methods, including both local and remote logons.

Privacy and Security Notice Section

AC.L2-3.1.9

Systems must display the following notice upon login:

Information system usage may be monitored or recorded, and is subject to audit. Unauthorized use of the information systems is prohibited. Unauthorized use is subject to criminal and civil penalties. Use of the information system affirms consent to monitoring and recording. The information system contains CUI with specific requirements imposed by the Department of Defense. Use of the information system may be subject to other specified requirements associated with certain types of CUI such as Export Controlled information.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Session Lock Section

AC.L2-3.1.10

The period of inactivity after which the system initiates a session lock is defined as no more than sixty (60) minutes.

Automatic session locking must occur after no more than sixty (60) minutes of user inactivity. Users must also be able to manually lock their sessions to secure their systems when leaving their workstations. Enforcing session locks ensures that unattended systems do not become vectors for unauthorized access.

Pattern-hiding session locks must be enabled on all devices within the system boundary to prevent unauthorized viewing of sensitive information on unattended systems. When sessions are locked, all previously visible information must be concealed. Re-authentication using approved credentials must be required to regain access to a locked session.

Session Termination Section

AC.L2-3.1.11

The conditions requiring a user session to terminate are defined as a period of user inactivity. This period is defined as no more than sixty (60) minutes.

User sessions must be automatically terminated after the defined period of inactivity to reduce the risk of unauthorized access to systems and data. All systems within the enclave must be configured to log off users after no more than sixty (60) minutes of inactivity. All systems within the enclave must be configured to automatically cancel the entire session once the inactivity threshold is reached. Session termination settings must be enforced consistently across all platforms and technologies in use. These measures help ensure that unattended sessions do not become a vector for unauthorized access to CUI.

Systems that cannot meet the inactivity timeout requirement must be reviewed and approved by the Cybersecurity Program Director. Approval is contingent upon: (a) a documented session termination method must be included in the System Baseline Standard, and (b) the system must be configured to enforce the alternative termination method reliably.

Controlling Remote Access Section

AC.L2-3.1.12

Remote access sessions are permitted. Permitted remote access session types must be identified in the System Catalog. When using a personal device or a device not authorized to store CUI, the system boundary must be defined at the session level, such as through a managed browser or virtual machine interface. These sessions must be protected to prevent the transfer of CUI to the local device and must be encrypted to prevent unauthorized access or interception.

If a system type is not listed as authorized for remote access in the System Catalog, the system must be configured to automatically block any attempt to establish a remote connection. Systems that do not meet baseline standards must not be allowed to connect.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Remote Access Confidentiality Section

AC.L2-3.1.13

Cryptographic mechanisms must be used to protect remote access sessions to ensure the confidentiality of data transmitted over external networks. All remote access endpoints must be configured to require encryption for remote sessions. Unencrypted access methods must be disabled, and only approved cryptographic protocols must be allowed. Cryptographic configurations must be reviewed to ensure alignment with current threat models and best practices.

Cryptographic mechanisms used to protect CUI must be validated under FIPS 140-2 or its successor standard. Only FIPS-validated cryptographic modules must be used when encrypting CUI during remote access sessions. Cryptographic modules must be selected from the NIST Cryptographic Module Validation Program (CMVP) list and configured in FIPS mode when applicable.

Remote Access Routing Section

AC.L2-3.1.14

The use of VPNs or SWGs is not permitted. Remote access may only be routed to the managed access control point maintained by the cloud provider.

Privileged Remote Access Section

AC.L2-3.1.15

The environment is cloud-based, and all administrative access is performed remotely. Remote access to all system security-relevant information is authorized for approved personnel. Security-relevant information includes system logs, configuration files, access control settings, audit records, and any data used to monitor or manage system security. Privileged commands shall be permitted to be executed through secure remote access mechanisms. All remote execution of privileged commands must be actively monitored and logged to maintain accountability and prevent misuse.

Wireless Access Authorization Section

AC.L2-3.1.16

There are no managed devices capable of connecting to wireless access in the scope of the program.

Wireless Access Protection Section

AC.L2-3.1.17

No wireless infrastructure may be deployed or enabled within the primary worksites. Organizational devices are not permitted to connect to any wireless access points. Wireless technologies introduce vulnerabilities such as unauthorized access, signal interception, and exploitation through rogue access points. By enforcing a strict prohibition of wireless access points, the organization significantly reduces its wireless attack surface and strengthens its overall security posture.

Mobile Device Connections Section

AC.L2-3.1.18

Mobile devices (smartphones, tablets, e-readers, etc.) are not permitted in the environment. Mobile platforms pose higher security risks due to their portability. This restriction applies to both organizationally owned and personally owned devices. The restriction reduces the risk of data leakage, unauthorized access, and loss or theft of sensitive information.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Encrypt CUI on Mobile Section

AC.L2-3.1.19

Mobile computing platforms (laptops, etc.) and mobile devices (smartphones, tablets, e-readers, etc.) are not permitted in the environment. Mobile platforms pose higher security risks due to their portability. This restriction applies to both organizationally owned and personally owned devices. The restriction reduces the risk of data leakage, unauthorized access, and loss or theft of sensitive information.

External Connections Section

AC.L2-3.1.20

Connections and the use of external systems must be controlled and verified. All external systems must be inventoried in the System Security Plan. This inventory serves as the authoritative record of external systems that interact with or impact the controlled environment. Each entry in the System Security Plan must include a justification for use. This ensures that all external connections are intentional, necessary, and documented in a manner that supports risk assessment and compliance oversight.

Connections to, and the use of, external systems must be verified to confirm that they are authorized and properly managed. Any changes to the external system list, such as the addition or removal of systems, must be verified through signatures on the Change Control Request Form. This process ensures accountability and traceability for all modifications involving external systems.

Portable Storage Use in External Systems Section

AC.L2-3.1.21

The use of portable storage media is strictly prohibited to minimize the risk of data leakage, unauthorized access, and the introduction of malicious code into organizational systems. This restriction applies to all forms of portable media, including USB flash drives, external hard drives, SD cards, and other removable storage devices.

Controlling Public Information Section

AC.L2-3.1.22

Sensitive information, including CUI, must not be released onto publicly accessible systems. These systems, which are accessible to the public without identification or authentication, must be strictly controlled to prevent unauthorized disclosure of nonpublic data. This includes websites, social media platforms, and other digital channels that are not restricted to internal or authorized users. To ensure compliance, all content intended for publication on publicly accessible systems must be reviewed to confirm that it does not contain CUI or other protected information. This review process must be logged, and occur both before and after publication to maintain ongoing oversight and accountability. Self-review is permitted.

Individuals authorized to post content on publicly accessible systems must be identified in the User, Process, and Asset Inventory. These individuals must be designated as "Authorized Publishers" and are responsible for ensuring that only approved and properly reviewed content is submitted for public access. In addition, individuals authorized to review content before and after publication must also be identified in the User, Process, and Asset Inventory. These individuals must be designated as "Authorized Publication Reviewers." Reviewers must complete the Publication Review Log both prior to and following publication to document the review process and confirm compliance.

All publicly accessible systems that are authorized for organizational publications must be inventoried and documented in the User, Process, and Asset Inventory. Each entry in the inventory must include detailed procedures for removing published content from the system if necessary. These procedures must include initiation of the Incident Response Plan to ensure that any improper or unauthorized disclosures are addressed through formal incident response protocols.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.2 Awareness and Training Policy

The purpose of the Awareness and Training policy is to ensure that all users of our systems (including subcontractors and other guest accounts), and all employees and subcontractors, are aware of their obligations regarding their use, as well as their obligations regarding the protection of sensitive data in digital and physical forms.

Role-Based Risk Awareness Section

AT.L2-3.2.1

Security risks associated with organizational activities involving CUI must be clearly identified and communicated to all personnel through role-appropriate documentation. These risks must be explicitly outlined in both the Acceptable Use Policy and the Privileged User Acceptable Use Policy. This ensures that all users, regardless of their level of access, are made aware of the potential threats and responsibilities associated with their roles. Managers, system administrators, and general users must be made aware of the security risks related to their activities and the applicable policies, standards, and procedures that govern the secure use of organizational systems. This awareness is foundational to reducing human error and strengthening the overall security posture of the environment.

The training catalog, and record of training completion must be inventoried in the User, Process, and Asset Inventory or other training record system. Users must complete training before accessing the system, and annually thereafter.

All relevant organizational policies, standards, and procedures must be documented within the Acceptable Use Policy and the Privileged User Acceptable Use Policy. Including this information in both policies ensures that users at all levels have access to the guidance necessary to perform their duties securely and in compliance with federal requirements.

All personnel must sign the Acceptable Use Policy as a condition of access to organizational systems. This signature serves as formal acknowledgment that the individual understands the security risks, responsibilities, and behavioral expectations associated with their role. It also reinforces accountability and supports enforcement of disciplinary actions in the event of policy violations. Signing this policy affirms that privileged users understand the heightened responsibilities and potential consequences of misuse.

Role-Based Security Training Section

AT.L2-3.2.2

Personnel roles must be formally assigned in the User, Process, and Asset Inventory. These assignments must be traceable to individuals and aligned with their job functions and system access levels.

All users must complete DoW CUI and cybersecurity awareness training to ensure they understand the risks associated with their roles and the systems they access. This training must be conducted at onboarding and refreshed at regular intervals, or when roles change, to maintain awareness of evolving threats and responsibilities. The content and frequency of training must be determined based on the sensitivity of the systems accessed and the potential impact of user actions. Training records must be maintained to demonstrate compliance and support audits or assessments.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Insider Threat Awareness Section

AT.L2-3.2.3

Potential indicators associated with insider threats must be identified and communicated to all users as part of the security awareness program. These indicators include, but are not limited to: inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, rules, or practices. These behaviors must be treated as potential precursors to insider threats and must be addressed through both proactive monitoring and user education. Personnel must be made aware of how to recognize these behaviors and the appropriate channels for reporting them in accordance with established procedures.

All users must complete Insider Threat Awareness Training. Required training is documented in the User, Process, and Asset Inventory or other training tracking system. Training must include guidance on how to report concerns through secure and confidential channels, and how to respond appropriately if an insider threat is suspected. Completion records must be maintained to demonstrate compliance and support audits.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.3 Audit and Accountability Policy

The purpose of the Audit and Accountability policy is to ensure that we capture the information needed to validate the proper use of our systems and compliance with our processes. The policy also dictates our approach to capturing historical information of system activity for the purpose of investigating security events.

System Auditing Section

AU.L2-3.3.1

Audit logging shall be implemented across all organizational systems to ensure the ability to monitor, detect, and respond to security-relevant events. Logging mechanisms must be configured to capture sufficient detail to support accountability, incident investigation, and operational oversight.

Retention requirements for audit records are defined as no less than ninety (90) days, in accordance with organizational retention policies and applicable regulatory requirements.

User Accountability Section

AU.L2-3.3.2

Audit logs must be configured to accurately trace user activity to individual accounts to ensure accountability and support forensic investigations. Each user shall be assigned a unique identifier during the account creation process, which must be used to associate all system actions with the responsible individual. Logs must be traceable to user accounts at all times, enabling the organization to detect unauthorized activity, investigate incidents, and maintain a secure operating environment.

Event Review Section

AU.L2-3.3.3

Audit log review processes shall be conducted on a recurring basis to ensure the integrity, relevance, and effectiveness of logged security events. Logged events must be reviewed quarterly to identify indicators of compromise, unauthorized activity, or anomalies that may require further investigation. False positives logic must be evaluated during each review cycle for accuracy and adjusted as necessary to reduce the frequency of irrelevant or misleading alerts. This ensures that security personnel can focus on actionable events and maintain operational efficiency.

Event types being logged must be assessed quarterly for necessity and relevance to ensure that audit logs capture meaningful data aligned with organizational risk tolerance and compliance requirements. Changes to audit log configurations, including modifications to event types or filtering logic, must be documented and tracked through a pre-approved change case. These practices ensure that all changes are authorized, traceable, and aligned with established change management procedures.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Audit Failure Alerting Section

AU.L2-3.3.4

Audit logging mechanisms must be continuously monitored to ensure they are functioning as intended and capturing required security-relevant events. Routine monitoring is essential to detect logging failures that could compromise the organization's ability to trace system activity and respond to incidents. Systems must be configured to automatically detect and report failures in the audit logging process, including interruptions, misconfigurations, or storage limitations that may prevent logs from being generated or retained.

The Defend Team must be notified in the case of an audit logging failure. Designated individuals must be promptly notified in the event of a logging failure to ensure timely investigation and remediation. System configurations that generate alerts to the Technical Lead and/or the Cybersecurity Program Director in the event of audit process failures shall be documented in the System Baseline Standard.

Audit Correlation Section

AU.L2-3.3.5

To support effective detection and investigation of suspicious activity, the organization must perform log aggregation to centralize audit records from across systems. Centralized logging enables the correlation of events across multiple sources, which is essential for identifying patterns of unauthorized or anomalous behavior.

The system used for monitoring and analysis must include the following capabilities: ingest logs from all relevant systems within the organization; correlate anomalies across different systems to identify patterns or coordinated activity; analyze anomalies and generate reports for review by security personnel; detect indicators of potential attacks, including lateral movement or privilege escalation; monitor communications for signs of unauthorized access or data exfiltration; analyze logs to detect unauthorized use of systems or data; and alert designated personnel when urgent or high-risk issues are identified.

Reduction and Reporting Section

AU.L2-3.3.6

Audit record reduction capabilities must be implemented to transform raw audit logs into meaningful, structured data that supports efficient analysis. These capabilities should enable both real-time and historical analysis to facilitate timely detection of security-relevant events and support forensic investigations. Audit data must be ingested, normalized, and correlated to identify significant patterns and anomalies across diverse data sources. Additionally, systems must provide on-demand report generation to support operational, compliance, and investigative needs.

Authoritative Time Source Section

AU.L2-3.3.7

Systems must be configured to use an internal authoritative source for time-stamping audit records. In addition, systems must synchronize internal system clocks with an established external authoritative time source. Accurate and consistent timekeeping is essential for ensuring the integrity and correlation of audit logs across systems.

The organization shall define the authoritative time source for each system in the System Catalog. The specific time source used for each system must be documented in the System Catalog.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Audit Protection Section

AU.L2-3.3.8

Audit log information and audit log tools must be protected from unauthorized access, modification, and deletion. Select personnel must be formally designated and authorized to perform audit logging roles, duties, and responsibilities. Only individuals with explicit authorization shall be assigned to auditing roles.
Audit logging roles include, but are not limited to: configuring audit settings, managing audit log storage, and reviewing audit records for indications of suspicious or unauthorized activity.

Audit logging privileges must be assigned based on the principle of least privilege, ensuring individuals are granted only the minimum access necessary to fulfill their responsibilities. A defined subset of roles shall be configured with the authority to review and analyze audit information and manage logging tools. Separation of duties must be maintained to reduce the risk of unauthorized changes and to support the integrity of the audit process. The number of users authorized to modify auditing settings must be minimized. These individuals must be identified and listed separately in the privileged account list to ensure visibility and accountability.

Audit Management Section

AU.L2-3.3.9

To ensure proper role assignment and authorization, the organization must restrict the management of audit logging functionality to a defined subset of privileged users. Only individuals who have received explicit authorization are permitted to manage or review audit logs. Roles that are permitted to manage audit logging functionality are documented in the roles section of the SSP.

In alignment with privilege management and the principle of least privilege, audit logging roles must be assigned based on clearly defined job responsibilities and the minimum level of access required to perform those duties effectively. Individuals responsible for audit logging functions must be granted only the privileges necessary to fulfill their responsibilities. Furthermore, roles responsible for reviewing audit logs must be distinct from those authorized to configure or manage audit logging settings to maintain separation of duties.

Access control and oversight must be maintained by configuring a select subset of roles to review and analyze audit logs and operate logging tools. This ensures that oversight is both effective and limited to trusted personnel. The number of users with the ability to modify audit logging configurations must be kept to the absolute minimum necessary for operational needs. Users with elevated privileges to change audit logging settings must be explicitly identified on the privileged account list to support oversight and auditing efforts.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.4 Configuration Management Policy

The purpose of the Configuration Management policy is to establish and harden system configuration baselines. Systems with baseline configurations are easier to maintain, as any performance issues should be addressable by returning to baseline or modifying the baseline. They are also easier to secure, because it is easier to detect anomalous behavior on a baselined system. In addition, the CM policy defines the processes necessary to manage and modify system baselines.

System Baselining Section

CM.L2-3.4.1

A System Baseline Standard must be created and maintained to document baseline configurations for all systems. These baselines represent the approved, secure configurations that systems must adhere to throughout their lifecycle. The System Baseline Standard must include detailed specifications for each baseline. Baseline configurations must be formally reviewed, approved, and serve as a reference point for detecting unauthorized changes or deviations.

A User, Process, and Asset Inventory must be created to maintain an up-to-date inventory of individual assets within the environment. This inventory must include specifications for each asset, such as hardware type, software versions, firmware, and associated documentation. The User, Process, and Asset Inventory and System Baseline Standard must be maintained continuously to reflect changes in the environment, ensuring accurate and current records for all systems and components.

Security Configuration Enforcement Section

CM.L2-3.4.2

Security configuration settings must be established and enforced for all information technology products used within systems. These settings are essential to ensure systems are hardened against known vulnerabilities and misconfigurations.

Assets must be configured according to system baselines defined in the System Baseline Standard. These baselines represent the approved, secure configurations for each system type. The System Baseline Standard must contain the security configurations for all systems, including operating systems, applications, and network devices, to ensure consistent protection across the enterprise. This approach ensures that all systems begin from a known, secure state, reducing the risk of unauthorized changes and improving the ability to detect and respond to deviations. NIST SP 800-70 and SP 800-128 provide further guidance on security configuration settings.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Change Management Section

CM.L2-3.4.3

A formal Change Management Process must be established and maintained to ensure that all system changes are properly controlled, evaluated, and documented in alignment with security and operational requirements. The change management process must support the integrity of system baselines and ensure that all changes are subject to appropriate security-focused oversight. System changes must be tracked, reviewed, approved or denied, and logged in accordance with the established Change Management Process. Any changes to approved configuration baselines must be submitted through the Case Management System, which provides traceability and accountability for all modifications.

The Change Management Board (CMB) reviews change control cases as they are opened, and meets if required. The board is led by the Cybersecurity Program Director (CPD), and shall include the Technical Lead, Defend Team, and Harden Team to ensure multidisciplinary oversight. All proposed changes must be reviewed and approved by the CMB prior to implementation. This review shall include an evaluation of the potential security impact and alignment with the organization's risk tolerance. The Change Management Board may preapprove certain types of changes. Requests for pre-approved changes are documented in a change control case. Small, low risk changes to the baseline may be preapproved. Critical security patches are always pre-approved.

Security Impact Analysis Section

CM.L2-3.4.4

A Security Impact Analysis (SIA) must be conducted prior to implementing any configuration or system changes. The SIA must evaluate whether the proposed change introduces new security risks or affects existing controls. Identified risks must be clearly documented and either mitigated through appropriate safeguards or formally accepted by authorized personnel. This process aligns with guidance from NIST SP 800-128, which outlines best practices for conducting security impact analyses as part of a comprehensive configuration change management program.

The results of the SIA must be incorporated into the change management process. No changes may proceed without a completed and reviewed SIA. All SIAs must be retained as part of the change record and referenced in the Case Management System.

Access Restrictions for Change Section

CM.L2-3.4.5

Physical Controlled Unclassified Information systems are not permitted in the environment. All CUI data must remain in secure cloud environments.

Logical access restrictions must be implemented to prevent unauthorized individuals from logging into systems for the purpose of making configuration changes. This includes, but is not limited to, requiring specific credentials or elevated permissions to modify configuration settings, apply software patches, or update system libraries. Technical enforcement mechanisms such as access control lists, role-based access permissions, and system-level authentication requirements must be used to ensure that only authorized users are able to access or modify configuration components. All access to configuration settings and any resulting changes must be logged in a secure and auditable manner.

Enforcement of access restrictions must be integrated into the IT ticketing resolution workflow. This ensures that access permissions are validated and applied in accordance with approved change requests.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Least Functionality Section

CM.L2-3.4.6

Organizational systems must be configured according to the principle of least functionality, ensuring that only essential capabilities are enabled and all unnecessary features are removed or disabled. This approach reduces the system's attack surface and limits opportunities for exploitation by minimizing the number of active services, applications, and components.

Essential capabilities for each system must be defined and documented in the System Catalog. This catalog must serve as the authoritative source for identifying the specific functions required for each system to support its mission or business purpose.

Nonessential Functionality Section

CM.L2-3.4.7

Programs are defined as software that runs on endpoints.
Common examples of programs include Microsoft Word, or File Explorer
Essential programs are defined as programs that support business needs, practices, or processes.
Nonessential programs are defined in the System Catalog on a per-system basis.
Nonessential programs must be disabled or restricted within the established boundary.

Functions are defined as capabilities provided by the system.
Common examples of functions include Cortana, or Bluetooth advertising.
Essential functions are defined as functions that support business needs, practices, or processes.
Nonessential functions are defined in the System Catalog on a per-system basis.
Nonessential functions must be disabled or restricted within the established boundary.

Ports are defined as a numbered logical endpoint that identifies a specific process or service in network communications.
Common examples of ports are Port 443 for HTTPS or Port 80 for HTTP.
Essential ports are defined as ports that support business needs, practices, or processes.
Nonessential ports are defined in the System Catalog on a per-system basis.
Nonessential ports must be disabled or restricted within the established boundary.

Protocols are defined as a standardized set of rules and conventions that define how data is formatted, transmitted, received, and interpreted between communicating devices on a network.
Common examples of protocols include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
Essential protocols are defined as protocols that support business needs, practices, or processes.
Nonessential protocols are defined in the System Catalog on a per-system basis.
Nonessential protocols must be disabled or restricted within the established boundary.

Services are defined as background processes that run on endpoints.
Common examples of services include BitLocker Drive Encryption Service, or the Microsoft Defender Antivirus Service.
Essential services are defined as services that support business needs, practices, or processes.
Nonessential services are defined in the System Catalog on a per-system basis.
Nonessential services must be disabled or restricted within the established boundary.

This policy is established in accordance with CMMC Assessment Guide, CM.L2-3.4.7 Nonessential Functionality, which may be reviewed for further implementation guidance.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Application Execution Policy Section

CM.L2-3.4.8

The organization must maintain a list of unauthorized software and block it from executing on organizational systems. The list is referred to as a software deny list. The software deny list is contained in the System Catalog. The software specified is not permitted to install or execute on fully managed organization systems. This enforcement must be achieved through technical controls such as endpoint protection platforms, group policy restrictions, and application control tools.
This policy is established in accordance with CMMC Assessment Guide, CM.L2.3.4.8 Application Execution Policy, which may be reviewed for further implementation guidance.

Software Installation Section

CM.L2-3.4.9

Users are permitted to install software not present on the organization denylist.

Unapproved software discovered during security monitoring must be documented in a security monitoring case.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.5 Identification and Authentication Policy

The purpose of the Identification and Authentication Policy is to define the rules for managing password and other authentication mechanisms (including multi-factor authentication) that support access control policies and enhance the ability to connect users to system actions.

Identification Section

IA.L2-3.5.1

All users, processes acting on behalf of users, and devices accessing the system must be uniquely identified before access is granted. Unique identification ensures that each system interaction can be traced to a specific individual, process, or device, supporting accountability and auditability. Accurate identification supports the enforcement of least privilege by ensuring that access is granted only to known and authorized entities.

An inventory of all users, processes, and devices must be maintained and recorded in the User, Process, and Asset Inventory. The inventory must include relevant attributes such as user IDs, device identifiers, roles, and associated access privileges. Keeping this inventory current is essential for maintaining visibility into system access and ensuring that only authorized entities are permitted.

Authentication Section

IA.L2-3.5.2

All organizational information systems must be configured to require authentication before granting access to any system resources. These authentication requirements must apply to all access types, including both local and remote connections, and covers users, service principals, processes, or devices. No access to system resources shall be permitted unless the entity requesting access has successfully completed an authentication process using an approved mechanism. Enforcing authentication before access ensures that only verified users, service principals, processes, or devices are allowed to interact with system resources, thereby supporting identity-based access control.

Authentication mechanisms must be implemented in accordance with organizational security policies and procedures. These mechanisms must be capable of reliably identifying and verifying the identity of users, service principals, processes, or devices. The authentication process must support the enforcement of access controls based on verified identity, ensuring that only authorized entities are granted access to the specific resources they are permitted to use. These authentication requirements shall be designed to protect CUI by ensuring that only authenticated and authorized entities can access sensitive systems and data.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Multifactor Authentication (MFA) Section

IA.L2-3.5.3

To protect sensitive systems and data, multi-factor authentication (MFA) must be implemented for the following types of access: local privileged access, which requires MFA for all users with elevated privileges who access systems directly through local interfaces, including administrators and other personnel authorized to perform security-critical functions; networked privileged access, which requires MFA for all privileged users accessing systems over a network, including administrative access to servers, network devices, and other critical infrastructure, whether accessed internally or remotely; and networked non-privileged access, which requires MFA for all non-privileged users accessing systems over a network, including general user access to enterprise applications, email, and file systems through internal networks or remote access solutions.

MFA must use at least two of the following distinct authentication factors: something the user knows (e.g., password or PIN), something the user has (e.g., smart card, security token), and something the user is (e.g., biometric identifier). Each factor must be independent to ensure that the compromise of one does not affect the integrity of the others. MFA solutions must be configured to prevent unauthorized access and support secure authentication across all access types.

Replay-Resistant Authentication Section

IA.L2-3.5.4

Authentication mechanisms for network access to privileged and non-privileged accounts must be designed and implemented to be resistant to replay attacks. Replay attacks occur when an adversary intercepts and reuses valid authentication data to gain unauthorized access. Replay-resistant authentication ensures that credentials cannot be captured and reused by malicious actors, preserving the integrity of the authentication process.

Authentication protocols must incorporate mechanisms such as nonces, timestamps, or cryptographic challenges. These methods ensure that each authentication attempt is unique and cannot be replicated by an attacker. Systems that do not support replay-resistant authentication are not permitted in the enclave due to the security risks they pose.

Identifier Reuse Section

IA.L2-3.5.5

The period within which identifiers cannot be reused is defined as forever.

All user, group, and device globally unique identifiers (GUIDs), also known as Object IDs, must be unique, non-reusable, and permanently maintained to ensure accountability and traceability within information systems. Identifiers must not be reused or deleted, even after a user account is deactivated or no longer in use. The Object ID serves as a persistent identifier that remains associated with the user throughout the lifecycle of their account. The system vendor is responsible for assigning each user a unique Object ID by default. The use of immutable and non-reusable identifiers ensures that historical records remain accurate and that access control decisions are based on reliable identity data.

In the event that a system does not support GUIDs, administrators must assign a unique identifier for each user, service principal, and asset. These identifiers must not be reused.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Identifier Handling Section

IA.L2-3.5.6

The period of inactivity after which an identifier is disabled is defined as no more than sixty (60) days.

User identifiers must be disabled after no more than sixty (60) consecutive days of inactivity to maintain access control integrity and reduce the risk of unauthorized access. Account status must be reviewed regularly to ensure compliance with inactivity thresholds.

Exceptions to this policy are permitted in the event a stale account must remain active for a business need. Exceptions are recorded in the User, Process, and Asset Inventory.

Password Complexity Section

IA.L2-3.5.7

Password complexity requirements are defined as a length of no less than eight (8) characters.
Password change of character requirements are defined as no less than one (1) character.

All system password enforcements must comply with the defined complexity and character requirements to strengthen defenses against unauthorized access and password-based attacks.
Users are permitted to use their current password when using a voluntary "forgot password" reset.

Password Reuse Section

IA.L2-3.5.8

The number of generations during which a password cannot be reused is specified as no less than one (1) generation.

Systems must be configured to prevent the re-use of a previous password when a password change is forced by an administrator.

In cases where a user forgets their password and initiates a reset, the system may allow the reuse of the most recent password, as it is still an acceptable, current password.

Temporary Passwords Section

IA.L2-3.5.9

Systems must be configured to enforce a mandatory password change upon first login when a temporary password is used. Enforcing a password change ensures that the temporary credential is replaced with a user-defined password that meets the complexity and reuse policies.

Temporary passwords are typically issued during initial account provisioning or password recovery scenarios. If systems do not support automatic prompting for password changes, administrators must manually reset the temporary password and coordinate with the user to complete the update. Implementation must be validated to ensure consistent enforcement across all platforms.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Cryptographically-Protected Passwords Section

IA.L2-3.5.10

Passwords must be protected during both storage and transmission to prevent unauthorized access and ensure confidentiality. Systems that do not implement password hashing by the vendor are not permitted. Password hashing must be managed by the vendor using strong cryptographic algorithms to secure stored credentials. Password protection during transmission is not inherited and must be addressed separately. When transmitting temporary passwords, encrypted email must be used to ensure confidentiality during delivery. All other password transmissions must either be avoided or managed through secure, vendor-provided authentication mechanisms.

Obscure Feedback Section

IA.L2-3.5.11

Authentication mechanisms must be configured to obscure authentication information. Passwords and other sensitive credentials must be masked or hidden as they are entered, typically using placeholder characters such as asterisks or dots. Systems must not display authentication information in plaintext at any point during the authentication process. These protections help mitigate risks such as shoulder surfing, screen capture, and other forms of credential observation.

Authentication mechanisms must also be configured to return generic error messages that do not disclose whether the username, password, or other credential was incorrect. All error responses should indicate only that authentication has failed, without specifying the reason, to prevent information disclosure that could aid unauthorized access attempts. All systems must implement these measures consistently to maintain the confidentiality of authentication data.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.6 Incident Response Policy

The purpose of the Incident Response Policy is to provide the guidelines necessary to evaluate events that may suggest an Incident, declare Incidents when they occur, and take the right steps after declaring an Incident to report, mitigate, and close the incident.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Incident Handling Section

IR.L2-3.6.1

An incident-handling capability must be formally established and maintained to ensure timely detection, reporting, analysis, and response to cybersecurity events that may impact the confidentiality, integrity, or availability of CUI. This capability must be documented in an Incident Response Plan (IRP) and supported by trained personnel, defined roles, and appropriate technical tools. The IRP must integrate forensic techniques, as recommended in NIST SP 800-86, including preserving evidence, maintaining chain of custody, and conducting analysis that supports legal or disciplinary action. For environments with mobile assets, NIST SP 800-101 Rev. 1 provides additional guidance on mobile device forensics. In accordance with NIST SP 800-161 Rev. 1, incident-handling capabilities must include mechanisms to detect and respond to supply chain-related threat events, including monitoring third-party service providers and critical components for compromise.

The term "incident" must not be used prematurely, as it carries legal, regulatory, and contractual implications. Until legal counsel has reviewed the facts and authorized the classification, all anomalous or suspicious activity shall be referred to as a "suspected threat event." If legal counsel confirms that the event qualifies as an incident, the IRP must be activated.

The IRP must include a preparation phase, as outlined in NIST SP 800-61 Rev. 2. This phase includes defining roles and responsibilities, establishing communication protocols, conducting training, and ensuring readiness of tools and procedures. Preparation also includes legal coordination to ensure that incident terminology is used appropriately and in compliance with regulatory obligations.

Personnel must be trained to recognize and report suspected threat events. All users play an active role in the detection and reporting of suspected threat events. Users must immediately report anomalous system behavior, suspicious emails, unauthorized access indicators, or any activity that appears inconsistent with normal operations. Reports may be submitted through the IT ticketing system, direct communication with the Cybersecurity Program Director, or escalation through supervisors. User response activities include prompt reporting, participation in triage as requested, preserving potential evidence by not altering affected systems, and cooperating with the IR Team during analysis and containment. Users must not attempt self-remediation or deletion of artifacts. The IRP must define how user reports are received, escalated, and incorporated into the incident-handling process. This ensures that users are active participants in the detection and response lifecycle. User responsibilities are reinforced through onboarding training, annual refresher training, and security awareness communications. Training includes how to recognize indicators of compromise, how to report them, and expectations for user actions during each phase of the IR lifecycle.

Detection mechanisms must be in place to identify suspected threat events. These mechanisms may include automated monitoring systems, user reporting channels, and threat intelligence feeds. All detection capabilities must be configured to monitor activity across IP addresses, ports, and communication protocols to ensure comprehensive visibility. Upon detection of a suspected threat event, a formal Suspected Threat Event Process must be initiated. Designated senior personnel must conduct an initial review to determine whether there is reason to believe the activity is malicious. This analysis must be documented and must not result in the use of the term "incident" unless authorized by legal counsel.

The containment phase must include short-term and long-term strategies to limit the impact of the incident, isolate affected systems, and prevent further damage, as described in NIST SP 800-61 Rev. 2. The recovery phase must focus on restoring affected systems and services to normal operation. This includes validating system integrity, restoring from backups, and verifying that vulnerabilities have been addressed. Recovery procedures must be documented and tested annually at a minimum.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Incident Reporting Section

IR.L2-3.6.2

All security incidents must be documented and tracked to support forensic analysis, identify trends, and evaluate the effectiveness of incident response procedures. This includes capturing detailed information about the nature of the incident, affected systems, response actions taken, and any follow-up remediation. Maintaining a comprehensive incident history enables the organization to improve its detection and response capabilities over time. In alignment with guidance from NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, incident tracking should support the full lifecycle of incident response: preparation, detection and analysis, containment, eradication, recovery, and post-incident activity. This structured approach ensures that incident data is actionable and contributes to continuous improvement.

The organization must identify the authorities and organizational officials to whom incidents are reported. These individuals or roles must be listed in the User, Process, and Asset Inventory. This ensures that all reporting responsibilities are clearly defined and accessible during an incident. All incidents must be reported in accordance with the procedures outlined in the Incident Response Plan, including timelines, communication channels, and escalation paths. This ensures that internal and external stakeholders are informed appropriately and that regulatory or contractual obligations are met.

Incident Response Testing Section

IR.L2-3.6.3

Incident Response Plan testing must be conducted annually at a minimum to identify and remediate any weaknesses, gaps, or procedural issues that could hinder effective incident handling. Testing must involve all individuals and roles identified in the plan to ensure coordinated response capabilities across the organization. A tabletop exercise must be conducted simulating a realistic incident scenario. Participants must walk through their roles and responsibilities as outlined in the plan, discussing actions, decisions, and communication flows.

Upon completion of the exercise, a report must be generated documenting the scenario, participants, outcomes, and any issues or deficiencies identified during the simulation. If the exercise reveals the need for updates to the incident response plan, a formal change control request (CCR) must be submitted in accordance with the organization's change management process. All test results and corrective actions must be documented and retained for audit and continuous improvement purposes.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.7 Maintenance Policy

The purpose of the Maintenance Policy is to ensure that routine maintenance and break/fix work is performed on organizational systems in order to keep them operational, and that such work is conducted in a manner that limits the risk of system compromise and prevents unauthorized access to CUI.

Perform Maintenance Section

MA.L2-3.7.1

System maintenance must be performed to ensure continued system integrity, availability, and performance without introducing vulnerabilities. This includes deploying approved updates and restoring non-performing systems to a secure operational baseline. Maintenance must follow defined schedules or be initiated in response to system failures, ensuring systems remain functional and secure. All maintenance activities must be conducted using only approved software and hardware tools.

Systems used for maintenance are described in the System Baseline Standard.

Maintenance updates must be delivered through a centralized endpoint management platform that enforces update policies across all managed systems. These policies must define how and when systems receive and install both security and feature updates, including deferral periods, deadlines, active hours, and reboot behavior. These configurations must be designed to maintain security posture while minimizing operational disruption. Updates that are pre-approved through the organization's change management process shall be applied automatically to ensure timely patching of critical vulnerabilities.

System Maintenance Control Section

MA.L2-3.7.2

Controls over the tools, techniques, mechanisms, and personnel involved in maintenance activities must be implemented to ensure the security of Controlled Unclassified Information (CUI) during system maintenance. These tools and mechanisms must be approved prior to use and must be controlled and monitored during use. This helps prevent the introduction of malicious code or unauthorized functionality into the system environment.

Individuals from outside the organization may be granted privileged access to systems for maintenance purposes. Such access must be strictly controlled and supervised to ensure that only authorized personnel perform maintenance tasks. Access must be limited to the duration of the maintenance activity, and all external access must be terminated immediately upon completion.

Physical and logical access to maintenance tools, techniques, and mechanisms must be restricted to authorized maintenance personnel. The organization must ensure that maintenance tools do not remain connected to or accessible from the system once maintenance is complete.

External Service Providers with accounts on organization systems may activate their privileged roles.

Equipment Sanitization Section

MA.L2-3.7.3

No in-scope physical equipment containing Controlled Unclassified Information (CUI) is permitted, therefore, the requirements for sanitizing equipment prior to off-site maintenance do not apply.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Diagnostic Media Inspection Section

MA.L2-3.7.4

Removable media shall not be permitted in the environment. Therefore, media containing diagnostic and/or test programs shall be prohibited.

Nonlocal Maintenance Section

MA.L2-3.7.5

Nonlocal maintenance sessions include remote diagnostics, vendor support, or any administrative access performed over a network. To ensure secure access, multifactor authentication (MFA) must be enforced for all nonlocal maintenance sessions. Additionally, systems must be configured to require MFA before granting access to privileged accounts, reducing the risk of unauthorized administrative activity.

Systems must be configured to automatically terminate nonlocal maintenance connections once the session is complete. This helps ensure that remote access is not left open beyond its intended use.

Maintenance Personnel Section

MA.L2-3.7.6

If individuals outside the organization must be given access to organizational systems for maintenance, their actions must be closely monitored. External maintenance personnel, such as vendor technicians, must only be granted access when absolutely necessary and under strict oversight. Monitoring must include real-time observation, logging of all activities, and review of access records to ensure that no unauthorized actions are taken during the maintenance session. Remote maintenance sessions conducted by external personnel must be controlled through secure access methods, such as time-limited credentials, session recording, and multifactor authentication.

Maintenance personnel without required access authorization must be supervised during onsite maintenance activities. This includes ensuring that all individuals performing maintenance are escorted by authorized personnel at all times while in controlled areas. Maintenance personnel shall sign into controlled areas and are escorted by authorized individuals while inside the controlled areas. These procedures help prevent unauthorized physical access to sensitive systems and reduce the risk of data exposure or tampering.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.8 Media Protection Policy

The purpose of the Media Protection Policy is to ensure that systems including digital media and physical media containing FCI and CUI are properly identified, marked, safeguarded and disposed.

Media Protection Section

MP.L2-3.8.1

System media containing CUI is not permitted. This includes digital system media (e.g. hard drives, solid-state drives, USB flash drives, memory cards, CDs, and DVDs) and non-digital system media (e.g. printed documents, notebooks, photographs and microfilm).

Media Access Section

MP.L2-3.8.2

System media containing CUI is not permitted. This includes digital system media (e.g. hard drives, solid-state drives, USB flash drives, memory cards, CDs, and DVDs) and non-digital system media (e.g. printed documents, notebooks, photographs and microfilm).

Media Disposal Section

MP.L2-3.8.3

We rely on our Cloud Service Provider(s) to properly sanitize and destroy media containing CUI.

Media Marking Section

MP.L2-3.8.4

Media containing CUI shall be marked and distributed in accordance with federal guidelines. CUI labels must follow "CUI Notice 2019-01: Controlled Unclassified Information (CUI) Coversheets and Labels." Limited Distribution Statements can be found in the "Distribution Statements IAW DoDI 5230.24" publication. Guidance for CUI Marking can be found in the NARA CUI Handbook 2016-12-06. Personnel have the responsibility to ensure all media with CUI is clearly and properly marked. Personnel will ensure media with CUI is distributed following organizational guidelines and the DoD CUI Registry.

Media Accountability Section

MP.L2-3.8.5

System media containing CUI is not permitted. This includes digital system media (e.g. hard drives, solid-state drives, USB flash drives, memory cards, CDs, and DVDs) and non-digital system media (e.g. printed documents, notebooks, photographs and microfilm).

Portable Storage Encryption Section

MP.L2-3.8.6

The use of portable storage media is strictly prohibited to minimize the risk of data leakage, unauthorized access, and the introduction of malicious code into organizational systems. This restriction applies to all forms of portable media, including USB flash drives, external hard drives, SD cards, and other removable storage devices.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Removable Media Section

MP.L2-3.8.7

The use of portable storage media is strictly prohibited to minimize the risk of data leakage, unauthorized access, and the introduction of malicious code into organizational systems. This restriction applies to all forms of portable media, including USB flash drives, external hard drives, SD cards, and other removable storage devices.

Shared Media Section

MP.L2-3.8.8

The use of portable storage media is strictly prohibited to minimize the risk of data leakage, unauthorized access, and the introduction of malicious code into organizational systems. This restriction applies to all forms of portable media, including USB flash drives, external hard drives, SD cards, and other removable storage devices.

Protecting Backups Section

MP.L2-3.8.9

Physical backups for CUI are not permitted. Backups are only stored on cloud service providers.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.9 Personnel Security Policy

The Personnel Security policy aims to safeguard information by implementing appropriate screening procedures and taking necessary actions regarding personnel.

Personnel Screening Section

PS.L2-3.9.1

To ensure eligibility for access to Controlled Unclassified Information (CUI), the organization must verify that each individual is a U.S. person, as defined by applicable federal regulations. This verification is a prerequisite for granting access to CUI and is part of the organization's personnel screening requirements.

Before access to CUI is authorized, a third-party background investigation must be completed for each individual. This investigation must assess the individual's trustworthiness, reliability, and suitability for handling sensitive information. The organization must implement these screening requirements to ensure that only individuals with verified identity, demonstrated trustworthiness, and a legitimate, documented need are granted access to CUI.

Authorized holders of CUI must ensure that all intended recipients have a lawful government purpose before disseminating the information. This expectation must be reasonable and in accordance with 32 CFR 2002.16(c)(1). A lawful government purpose is defined in 32 CFR 2002.4(bb) as any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities, including those of non-executive branch entities such as state and local law enforcement.

Personnel Actions Section

PS.L2-3.9.2

A formal process for managing personnel termination and internal transfers must be established and documented. This process must define responsibilities, timelines, and procedures to ensure secure and consistent handling of CUI access and assets containing CUI. The Govern Team must notify the Technical Lead via an Identity and Access Management Case that a privileged account will be disabled and removed.

All access privileges assigned to an individual must be revoked immediately upon termination or departure from the organization to prevent unauthorized access to systems and data. When an individual is transferred to a different role or department, their access permissions must be reviewed and modified to reflect their new responsibilities. Access that is no longer required must be removed to enforce the principle of least privilege.

All organizational assets issued to the individual must be returned upon termination or departure. The return process must be documented and verified to ensure accountability. Organizational assets that must be recovered include, but are not limited to: computing endpoints such as laptops, desktops, and mobile devices; peripherals such as external drives, docking stations, and monitors; identification badges and access cards; and physical keys and security tokens.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.10 Physical Protection Policy

The purpose of the Physical Protection Policy is to ensure proper control, management, and monitoring of physical access to the organization's networks and physical CUI as appropriate.

Limit Physical Access Section

PE.L2-3.10.1

Controlled Unclassified Information (CUI) must not be stored or handled in any physical spaces. This restriction applies to all organizational systems, equipment, and operating environments. The intent is to eliminate the possibility of physical access to CUI, thereby reducing the risk of unauthorized exposure. Third party physical datacenter security is managed by the external service provider.

Monitoring the Facility Section

PE.L2-3.10.2

Controlled Unclassified Information (CUI) must not be stored or handled in any physical spaces. This restriction applies to all organizational systems, equipment, and operating environments. The intent is to eliminate the possibility of physical access to CUI, thereby reducing the risk of unauthorized exposure. Third party physical datacenter security is managed by the external service provider.

Escorting Visitors Section

PE.L2-3.10.3

The organization does not maintain any physical areas where CUI is present. If physical spaces containing CUI were present, then all visitors would require an escort. Third party physical datacenter security is managed by the external service provider.

Physical Access Logs Section

PE.L2-3.10.4

Controlled Unclassified Information (CUI) must not be stored or handled in any physical spaces. The intent is to eliminate the possibility of physical access to CUI, thereby reducing the risk of unauthorized exposure. Third party physical datacenter security is managed by the external service provider.

Managing Physical Access Section

PE.L2-3.10.5

Controlled Unclassified Information (CUI) must not be stored or handled in any physical spaces. The intent is to eliminate the possibility of physical access to CUI, thereby reducing the risk of unauthorized exposure. Third party physical datacenter security is managed by the external service provider.

Alternative Work Sites Section

PE.L2-3.10.6

No alternative worksites are present within the scope of the environment.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.11 Risk Assessment Policy

The Purpose of the Risk Assessment policy is to ensure that the proper risk evaluation, documentation, mitigation, and remediation steps are taken, leveraging the totality of the Cybersecurity Program to manage risk effectively as well as periodically identify both changes to risks and identify additional actions that can be taken to further reduce risk.

Risk Assessments Section

RA.L2-3.11.1

The frequency to conduct a risk assessment is defined as no more than one (1) year.

A risk assessment must be conducted at least annually to ensure ongoing awareness of the threat landscape. The assessment must identify user groups, facilities, and systems that support the mission of the organization. Risks that could compromise these activities and resources must be analyzed and documented, as well as proposed mitigations. A risk assessment must also be conducted whenever new threat intelligence is discovered that could affect the security posture. A risk assessment must be initiated when significant changes are made to User Communities, Locations, or Systems. The Risk Assessment must be documented.

Vulnerability Scanning Section

RA.L2-3.11.2

The frequency to scan for vulnerabilities in organizational systems and applications is defined as no more than thirty (30) days.

Organizational systems and applications must be configured to conduct vulnerability scans no more than every thirty (30) days to ensure timely identification of security weaknesses. For systems that are incapable of supporting automated scanning, manual vulnerability assessments must be conducted at the same minimum frequency to maintain consistent coverage.

All systems identified as requiring patches or remediation actions must have a corresponding case opened to ensure the issue is formally tracked, prioritized, and addressed. This proactive approach supports continuous monitoring and rapid response to emerging threats.

Vulnerability Remediation Section

RA.L2-3.11.3

Vulnerabilities must be remediated in a timely manner based on risk assessments. Critical vulnerabilities that pose an immediate and severe threat to organizational systems or Controlled Unclassified Information (CUI) must be remediated within 30 days from the time of discovery. High-risk vulnerabilities, which represent significant but less immediate threats, must be addressed within 60 days. Medium risk vulnerabilities must be addressed within 90 days and low risk vulnerabilities must be addressed within 180 days.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.12 Security Assessment Policy

The purpose of the Security Assessment policy is to ensure the proper steps to mitigate risks using the defined practices are specified via the CMMC program.

Security Control Assessment Section

CA.L2-3.12.1

The frequency of security control assessments is defined as at least every one (1) year.

The organization must conduct a Security Control Assessment (SCA) at least annually to evaluate the effectiveness of its security controls and ensure ongoing compliance with applicable standards. This self-assessment is a critical component of the organization's risk management strategy and is essential for maintaining the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI). As part of this review, the organization must re-evaluate the effectiveness of its processes to ensure they continue to meet regulatory and contractual requirements.

Any control or process found to be deficient must be submitted through the organization's change control process and documented on the Operational Plan of Action. The change control request must include a description of the issue, proposed corrective actions, and a timeline for resolution.

Operational Plan of Action Section

CA.L2-3.12.2

According to 32 CFR 170.4(b), an "Operational Plan of Action" is defined as "the formal artifact which identifies temporary vulnerabilities and temporary deficiencies (e.g., necessary information system updates, patches, or reconfiguration as threats evolve) in implementation of requirements and documents how they will be mitigated, corrected, or eliminated. The OSA defines the format (e.g., document, spreadsheet, database) and specific content of its operational plan of action. An operational plan of action does not identify a timeline for remediation and is not the same as a POA&M, which is associated with an assessment for remediation of deficiencies that must be completed within 180 days. (CMMC-custom term)"

As it is the responsibility of the OSA to define the "specific content of its operational plan of action" we choose to follow the CFR's definition of a "temporary deficiency:"

According to 32 CFR 170.4(b), a "Temporary deficiency" is defined as "a condition where remediation of a discovered deficiency is feasible, and a known fix is available or is in process. The deficiency must be documented in an operational plan of action. A temporary deficiency is not based on an 'in progress' initial implementation of a CMMC security requirement but arises after implementation. A temporary deficiency may apply during the initial implementation of a security requirement if, during roll-out, specific issues with a very limited subset of equipment is discovered that must be separately addressed. There is no standard duration for which a temporary deficiency may be active. For example, FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency. (CMMC-custom term)"

An Operational Plan of Action must be developed, and include the items required by 32 CFR 170.4(b).

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Security Control Monitoring Section

CA.L2-3.12.3

Security controls must be monitored on an ongoing basis to ensure they continue to operate effectively and as intended. This ongoing monitoring provides continued assurance that safeguards and countermeasures remain functional, reliable, and capable of protecting Controlled Unclassified Information (CUI).

A defined set of security controls is subject to monitoring on a monthly basis. These controls are identified and documented in the Security Control Monitoring Plan, which serves as the authoritative reference for the security control monitoring plan. The monitoring plan ensures consistency in how control effectiveness is evaluated and provides traceability for assessment purposes.

The monitoring process incorporates a variety of techniques, including automated alerting systems, audit log reviews, vulnerability scanning, configuration integrity checks, and manual verification procedures. These activities are conducted to validate that the selected controls are not only present but are also operating as expected within the system environment. Records of monitoring activities must be maintained to demonstrate that controls are being evaluated consistently.

System Security Plan Section

CA.L2-3.12.4

The frequency to update the system security plan is defined as no more than one (1) year.

A System Security Plan (SSP) must be developed, documented, and maintained. This plan serves as a comprehensive record of how security controls are implemented and maintained to protect CUI. NIST SP 800-18 provides further guidance on developing security plans.

The SSP must include a clearly defined description of the system boundaries. This description must identify all assets, components, and interfaces that fall within the scope of the system and are subject to protection. It must also delineate what is considered internal to the system versus what lies outside its boundary.

The SSP must describe the environment in which the system operates. This includes the physical infrastructure, logical architecture, and organizational context. The description must provide insight into the facilities, technologies, and operational conditions that support the system's functionality and security.

The SSP must explain how each applicable security requirement from NIST SP 800-171 is implemented within the system. This explanation must include the technical, administrative, and procedural measures that have been put in place to satisfy each requirement. The implementation details must be specific enough to demonstrate compliance and support traceability.

The SSP must describe any relationships or interconnections between the system and external systems, service providers, or third-party entities. This description must include the nature of each connection, the purpose it serves, and any associated security considerations.

The SSP must be formally documented in a structured and accessible format. It must be maintained as an official record that accurately reflects the current state of the system and its security posture. The documentation must be sufficient to support internal reviews, external assessments, and ongoing risk management activities.

The SSP must be reviewed and updated at least annually. Updates must occur whenever there are significant changes to the system, its environment, or the implementation of security controls. A process must be established and followed to ensure that the SSP remains current, accurate, and reflective of the system's operational reality.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.13 System and Communications Protection Policy

The purpose of the System and Communication Protection policy is to ensure that the organization is actively identifying, managing, and controlling all system and communication channels.

Boundary Protection Section

SC.L2-3.13.1

The organization must define external system boundaries and key internal system boundaries to ensure effective control and monitoring of communications. These boundaries must be clearly represented in the Scope Enclave Diagram, which is included in the System Security Plan. Systems that provide boundary protection, such as firewalls, routers, and cloud-based security services, must be documented in the System Baseline Standard. This documentation must include both physical devices (e.g., firewall appliances) and virtual/cloud-based boundary protection mechanisms.

The organization must monitor, control, and protect communications at the external system boundary to prevent unauthorized access and data exfiltration. Boundary protection mechanisms must include access control lists (ACLs), firewall rules, and interface restrictions that limit or prohibit unauthorized connections. The external boundary must be continuously monitored using appropriate tools and technologies to detect and respond to suspicious or unauthorized activity. These protections must be configured to enforce the organization's access control policies and support confidentiality and integrity of CUI.

The organization must also control and monitor communications at key internal system boundaries, especially between network segments with different security levels or functions. Internal boundary protection must be implemented using segmentation techniques such as VLANs, internal firewalls, and access control policies. Network traffic must be segmented, controlled, monitored, and protected using internal boundary devices to limit lateral movement and isolate sensitive systems.

Security Engineering Section

SC.L2-3.13.2

The organization does not develop software, therefore software development techniques that promote effective information security do not need to be identified or implemented.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Role Separation Section

SC.L2-3.13.3

User functionality and system management functionality must be separated to reduce the risk of unauthorized access and maintain the integrity of system operations. These functions typically involve elevated permissions and pose a higher risk if misused or compromised. This separation ensures that administrative capabilities are only accessible through controlled and monitored channels, reducing the attack surface and limiting the potential for accidental or malicious misuse.

User functionality is defined as any activity that does not require elevated or privileged access, such as accessing business applications, reading email, or browsing internal resources. System management functionality includes tasks that require privileged access.

Distinct privileged and non-privileged accounts must be implemented to enforce role separation. Privileged accounts are used exclusively for system administration tasks, while non-privileged accounts are used for general user activities. Personnel must not use privileged accounts for day-to-day user functions. Personnel must not use non-privileged accounts for system management.

Shared Resource Control Section

SC.L2-3.13.4

Systems must be configured and maintained to prevent unauthorized and unintended information transfer through shared system resources such as memory, cache, or processing components. These protections must ensure that one user or process cannot infer or access data belonging to another through shared hardware or software components.

Logical isolation techniques must be applied to prevent unintentional data exposure between users. These techniques must include memory clearing routines, session isolation, and secure multi-user operating system features that enforce strict process and memory separation.

Public-Access System Separation Section

SC.L2-3.13.5

No publicly accessible system components hosted by the organization are permitted.

Network Communication by Exception Section

SC.L2-3.13.6

Boundary protection devices and internal network boundary devices must deny all inbound and outbound network communications traffic unless explicitly permitted. Boundary protection devices must follow a "deny by default, allow by exception" approach.

To ensure default denial, the final firewall rule must be set as a "deny all" rule. Allowing by exception requires preceding firewall rules to explicitly define exceptions to the "deny all" policy. Firewall rules must be applied to addresses, ports, and protocols.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Split Tunneling Section

SC.L2-3.13.7

Tunneling technologies such as virtual private networks (VPNs) and secure web gateways (SWGs) are not permitted in the environment. As a result, split tunneling cannot occur.

Data in Transit Section

SC.L2-3.13.8

FIPS-validated cryptographic methods must be used to protect the confidentiality of CUI during transmission. This includes any transfer of CUI over internal or external networks, whether wired or wireless. The use of encryption ensures that CUI is not exposed to unauthorized access, interception, or tampering while in transit. Acceptable cryptographic methods must comply with FIPS 140-2 standards, which define the security requirements for cryptographic modules used by federal agencies.

Remote access sessions involving CUI must be encrypted using FIPS-validated cryptographic protocols. These protocols must be configured to enforce strong encryption and prevent fallback to insecure or non-validated algorithms. All remote access mechanisms must ensure that CUI remains protected from unauthorized disclosure throughout the session lifecycle, including authentication, data exchange, and session termination.

The organization has no physical facilities present, and alternative methods of physical protection are not authorized.

Connection Termination Section

SC.L2-3.13.9

The period of inactivity to terminate network connections associated with communications sessions is defined as no more than sixty (60) minutes.

This means that systems must automatically terminate network connections associated with communication sessions when the communication session is ended, or after no more than sixty (60) minutes to reduce the risk of unauthorized access. All systems within the enclave must consistently enforce this timeout policy for network connections associated with communication sessions. A dual-layered approach, combining automated session termination with user responsibility, ensures consistent enforcement and reduces risk.

Users must be informed of their responsibility to terminate communication sessions when duties are complete, especially in shared or public environments. The Authorized Use policy should emphasize the importance of this behavior as a complement to automated controls and a key part of security awareness.

Key Management Section

SC.L2-3.13.10

Cryptographic keys must be used when cryptography is employed to protect CUI. These keys are essential to ensuring the confidentiality, integrity, and authenticity of sensitive data. Cryptographic keys must be used whenever cryptographic mechanisms are applied, including but not limited to data-at-rest encryption, data-in-transit protection, and secure communications. The system must be configured to automatically manage cryptographic keys throughout their lifecycle. The lifecycle includes key generation, distribution, storage, access control, rotation, archival, and destruction. Automated key management systems must enforce policies that prevent unauthorized access, ensure timely key rotation, and support secure key recovery mechanisms.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

CUI Encryption Section

SC.L2-3.13.11

All systems that contain CUI must use encryption that is validated under the Federal Information Processing Standards (FIPS). CUI must be encrypted using FIPS-validated encryption when it is at rest, in transit, or being processed. Systems must be configured to enforce the use of FIPS-validated encryption by default to ensure consistent protection of CUI. Any cryptographic functions or modules that are not FIPS-validated must be disabled or restricted to prevent unauthorized or non-compliant encryption. When encryption is inherited from cloud service providers or third-party platforms, it must be verified that the cryptographic modules in use are FIPS-validated.

FIPS-validated encryption is defined as encryption performed by a cryptographic module that appears on the Cryptographic Module Validation Program (CMVP) list, which can be found at: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program. FIPS-validated cryptography requires that the cryptographic module be tested and validated to meet FIPS 140-2 requirements. Using an approved algorithm alone is not sufficient because the software or hardware module that implements the algorithm must also be independently validated under FIPS 140.

Collaborative Device Control Section

SC.L2-3.13.12

No collaborative computing devices are permitted for use in the scope of the environment. Collaborative computing devices include any microphones or cameras connected to the network and controlled by standard (non-privileged) users.

Mobile Code Section

SC.L2-3.13.13

Mobile code refers to software programs or scripts that are transmitted across a network and executed on a local system without explicit installation by the user. Common examples include Java, JavaScript, ActiveX, Flash, and VBScript. Mobile code can also be embedded in files, such as macros or attached to emails.

Mobile code must be recognized as both a functional necessity for modern web applications and a potential vector for malware and unauthorized system access. Improperly controlled mobile code can introduce vulnerabilities, compromise system integrity, and lead to data breaches.

Systems must be configured to prevent the execution of unauthorized or harmful executables to reduce the risk of inadvertently introducing malicious mobile code. This includes applying browser security settings, disabling unnecessary scripting capabilities, and enforcing execution policies that restrict mobile code to trusted sources. Execution of mobile code must be limited to approved environments and must comply with documented security configurations.

Monitoring systems must be configured to ingest logs that record the use of mobile code across the environment.

Voice Over Internet Protocol Section

SC.L2-3.13.14

We follow the NIST 800-58 definition for VOIP, which states "Voice over Internet Protocol (VOIP) refers to the transmission of speech across data-style networks."

Only FedRAMP authorized voice providers are permitted for use. VOIP is monitored via the logging of the installation of non-FedRAMP VOIP applications and controlled by the removal of unapproved applications.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Communications Authenticity Section

SC.L2-3.13.15

Systems must be configured to protect the authenticity of communication sessions to ensure secure and verifiable data exchange between endpoints. Secure communication protocols, such as Transport Layer Security (TLS), must be implemented to provide encryption, endpoint authentication, and session integrity. These protections are critical to prevent unauthorized interception, session hijacking, and man-in-the-middle attacks. Systems must enforce mutual authentication where applicable, validate digital certificates, and monitor session activity for anomalies or unauthorized access attempts.

Data at Rest Section

SC.L2-3.13.16

Endpoints that store data at rest are not permitted in the enclave.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

3.14 System and Information Integrity Policy

The purpose of the System and Information Integrity policy is to ensure that technology assets (e.g., desktops, software) that contain CUI are continuously monitored to detect violations of the authorized security state. Additionally, email, a common attack vector, is monitored and protected to detect malicious activity.

Flaw Remediation Section

SI.L2-3.14.1

The time within which to identify system flaws is specified as no more than sixty (60) days.
The time within which to report system flaws is specified as no more than sixty (60) days.
The time within which to correct system flaws is specified as no more than thirty (30) days for critical vulnerabilities.
The time within which to correct system flaws is specified as no more than sixty (60) days for high vulnerabilities.
The time within which to correct system flaws is specified as no more than ninety (90) days for critical vulnerabilities.
The time within which to correct system flaws is specified as no more than one hundred eighty (180) days for low vulnerabilities.

System flaws must be identified, reported, analyzed, and corrected within the defined remediation windows. Flaw identification includes vulnerability scanning, analyst review, vendor advisories, threat intelligence feeds, and automated alerting from endpoint security tools. Flaws requiring vendor patches must be monitored until an update becomes available.

Flaws must be evaluated to determine operational impact, risk to CUI, required compensating controls, and whether immediate containment actions are necessary. Patches and updates must be tested and validated before deployment.

Flaws must be communicated to responsible personnel, updates system baselines as needed, and verifies remediation through vulnerability rescanning or system evaluation. Automated vulnerability scanning tools must be used to detect newly disclosed flaws and to confirm the effectiveness of corrective actions.

If a flaw cannot be remediated within the defined period, it must be documented on the Operational Plan of Action.

Malicious Code Protection Section

SI.L2-3.14.2

Malicious code protection must be implemented to detect and prevent the execution of unauthorized code, including viruses, worms, Trojan horses, spyware, and other forms of malware. It is defined as software or built-in system configurations that scan for, detect, and respond to malware threats. These mechanisms must be capable of identifying malicious code introduced through various vectors, such as email attachments, web downloads, removable media, and network traffic. This control ensures that systems are protected from threats that could compromise data integrity, confidentiality, or availability.

Malicious code protection must be enabled on all systems within the enclave that are designated in the System Catalog as requiring such protection. Designated locations typically include system entry and exit points such as firewalls, email servers, web servers, workstations, and mobile devices. This targeted deployment ensures that protection is applied where it is most needed, without overextending resources or introducing unnecessary complexity.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Security Alerts & Advisories Section

SI.L2-3.14.3

The organization must conduct a regular News Review to monitor system security alerts and advisories, ensuring timely awareness and response to emerging threats. This review must include monitoring the sources identified in the Tesseract Intel Sources List, which may include government advisories, vendor bulletins, and industry-specific threat intelligence feeds. It must also include identifying relevant articles and summarizing them to determine whether response actions are required. If needed, cases must be opened to ensure appropriate actions are taken.

Article summaries must follow a structured format that includes the issue description, why the issue is important, how urgent the response actions are, our response actions, response actions you should take, and reference to a change request case, if applicable.

The organization must maintain a News Review Log that includes the date of review, the person who conducted the review, articles included in the Weekly Cyber Intel Newsletter, articles escalated to an Emergent Intel Advisory, whether the Weekly Cyber Intel Newsletter was sent that day, and whether an Emergent Intel Advisory was sent that day.

The Weekly Cyber Intel Newsletter must be sent at the end of each week to provide a consolidated view of relevant threats and organizational responses. The Emergent Intel Advisory must be sent the same day a critical issue is detected to ensure rapid awareness and action. All publications, including the Weekly Cyber Intel Newsletter and Emergent Intel Advisory, must follow the organization's publication review process to ensure accuracy, clarity, and consistency.

Update Malicious Code Protection Section

SI.L2-3.14.4

Automated malware protection mechanisms must be configured to retrieve and apply updates automatically as soon as new releases become available. These updates include antivirus signature definitions, heuristic detection engines, and reputation-based threat intelligence. Because malware evolves rapidly, automated updates are essential to maintain the effectiveness of protection mechanisms and to reduce the window of exposure to new threats.

System & File Scanning Section

SI.L2-3.14.5

The frequency for malicious code scans is defined as no more than thirty (30) days.

Malicious code protection tools must be configured to perform real-time scans of files from external sources as they are downloaded, opened, or executed. This includes files received via email, web downloads, removable media, and other external vectors. These real-time scans must be enforced as part of the system's security configuration baseline, ensuring consistent protection across all endpoints and entry points. This proactive scanning approach helps detect and block threats before they can execute, reducing the risk of infection from zero-day malware, trojans, spyware, and other malicious code.

In addition to real-time scanning, systems must be configured to perform periodic scans of all files and directories to detect dormant or previously undetected malicious code. These scans must occur according to the frequency in the System Baseline Standard. Scheduled scans serve as a secondary layer of defense, helping to identify threats that may have bypassed initial detection or were introduced through less monitored channels.

Malicious code protection mechanisms must be integrated into the organization's security configuration baselines, ensuring they are consistently deployed and maintained across all systems. These tools must be capable of taking automated actions when threats are detected.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.

Presented by ardalyst™

Monitor Communications for Attacks Section

SI.L2-3.14.6

Organizational systems must monitor both internal system activity and external network communications to detect indicators of compromise, unauthorized access, or malicious behavior. This ensures comprehensive visibility across all operational environments. Security monitoring must be conducted on a daily basis. Implementing these practices enhances the organization's ability to respond swiftly to threats and maintain a strong cybersecurity posture.

Security monitoring must include analyzing alerts for indicators of potential attack. Monitoring shall be achieved through the deployment of Security Information and Event Management (SIEM) solutions. These SIEM solutions must aggregate logs from applications, network communications, and system components. Logs shall be continuously correlated, reviewed, and analyzed to identify patterns that may signal unauthorized activity or malicious behavior. Security monitoring personnel must open cases for suspected threat events. True positive suspected threat events must be considered for the initiation of the incident response plan.

Unauthorized Use Section

SI.L2-3.14.7

Authorized use is defined as all use permitted by the Cybersecurity Policy Manual.

When using organizational systems and devices, they may not be used:
- in any way that is against the law, including but not limited to activity such as gambling, piracy, child pornography, or the violation of copyright, trademark, or intellectual property laws;
- for the purpose of reverse engineering, copying, hacking, or otherwise modifying or competing with the organization;
- for the purpose of sending unsolicited email, SMS, or text (spam) messages, or for transmitting any viruses, worms, or other malicious or destructive code;
- for the purposes of, or while, impersonating any person or entity, or falsely stating or otherwise misrepresenting your affiliation with a person or entity;
- in any way that attempts to circumvent any billing mechanism;
- to stalk and/or harass another;
- to harm minors in any way;
- to resell services not authorized by the organization;
- by forging headers or otherwise manipulating identifiers to disguise the origin of any content;
- for any non-organization activities, such as the viewing of pornography, mining for bitcoin, etc.
- in a manner that misleads a third party into believing that they are interacting directly a third party that you do not have permission to represent;
- in a way that engages in any chain letters contests, junk email, pyramid schemes, spamming, surveys or other duplicative or unsolicited messages (commercial or otherwise);
- in any manner that could damage, disable, overburden or impair any organization server or the networks connected to any organization server, or compromise the ability of other users to access organization systems;
- to market any goods or services for any business purposes (including advertising and making offers to buy or sell goods or services), unless specifically allowed to do so by the organization;
- to transmit another's intellectual property or other proprietary or confidential information without such owner's or licensor's permission.

When using organizational systems, you must
- ensure that CUI is encrypted in process, storage and transit, including via email.

Additional acceptable use language can be found in the Acceptable Use Policy.

© Ardalyst Commercial, LLC.
Provided under license for internal use only.