**Current Implemented Controls**

**Access Controls**

* + 1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

**Access Control AC-2 Account Management**

**a. Defined and Documented Account Types**

**Implementation:**

* **User Accounts:** Regular accounts for employees have been defined and documented.
* **Administrative Accounts:** Privileged accounts for system administrators have been established.
* **Service Accounts:** Non-interactive accounts used by services or applications (e.g., Apache web server) have been configured.
* **Guest Accounts:** These are disabled by default and are only enabled when necessary, with strict expiration policies in place.
* **Prohibited Accounts:** We have defined and documented prohibited account types, such as shared user accounts, which are not allowed.

**b. Assigned Account Managers**

**Implementation:** Specific roles within the IT department have been assigned as Account Managers in Active Directory (AD). These individuals are responsible for the creation, management, and review of accounts, as outlined in the AD management policy.

**c. Established Group and Role Membership Prerequisites**

**Implementation:**

* **Departmental AD Groups:** Users are added to AD groups based on their department or role.
* **Role-Based Access Control (RBAC):** AD’s built-in RBAC features are utilized to ensure that users are only members of groups necessary for their job functions.

**d. Specified Authorized Users, Groups, Roles, and Access Authorizations**

**Implementation:**

* We have ensured that only valid, authorized users have accounts in AD, based on their employment status.
* Users have been assigned to appropriate AD groups that determine their access to resources, such as file shares, printers, or the Apache web server.
* Specific access authorizations and privileges have been defined using AD’s permissions model, which includes restricting certain groups from accessing sensitive servers or administrative tools.

**e. Established Approvals for Account Creation**

**Implementation:** A workflow has been established where account creation requests are submitted through a ticketing system. Approvals from department heads or IT managers are required before accounts are created in AD.

**f. Implemented Account Lifecycle Management (Creation, Modification, Disablement, Removal)**

**Implementation:**

* **Account Creation:** Accounts are created based on approved requests, following standard naming conventions.
* **Modification:** Changes to accounts, such as role changes or group membership, are logged and require approval.
* **Disablement:** Accounts are automatically disabled after a predefined period of inactivity or upon termination of employment.
* **Removal:** Accounts are removed from AD following a standard retention period after disablement, ensuring that all associated data is archived or transferred as necessary.

**g. Monitored Account Usage**

**Implementation:** Auditing has been enabled in AD to monitor account activities, including logon events, account creation, and changes to group memberships. Logs are forwarded to a SIEM system for real-time monitoring and alerts on suspicious activities.

**h. Set Up Notification of Account Changes**

**Implementation:** Automated notifications within the AD management system have been set up to alert account managers when:

* Accounts are no longer required.
* Users are terminated or transferred.
* There is a change in the user's role or system access needs. These notifications are sent within a predefined time period, typically within 24 hours of the change.

**i. Authorized System Access**

**Implementation:** System access has been authorized based on:

* **Valid Access Authorization:** Only users with proper authorization have been granted accounts.
* **Intended System Usage:** Access levels are aligned with the user’s role and their need for system resources.
* **Attributes:** Specific attributes, such as user department or security clearance, are considered when granting access.

**j. Conducted Account Review for Compliance**

**Implementation:** Regular (e.g., quarterly) reviews of all AD accounts are conducted to ensure compliance with account management policies. This review process includes checking group memberships, last login times, and account activity.

**k. Managed Change of Shared/Group Account Authenticators**

**Implementation:** For any shared or group accounts, a process has been established to change the account’s password or authenticator whenever a member leaves the group or no longer requires access.

**l. Aligned Account Management with Personnel Termination and Transfer Processes**

**Implementation:** AD account management processes have been integrated with HR’s termination and transfer workflows:

* **Immediate Disablement:** Upon notification from HR, the user’s AD account is immediately disabled.
* **Data Transfer:** Necessary data is transferred to a new owner, and the account is removed according to policy.
  + 1. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

**Access Control AC-3 Access Enforcement**

Implementation:

* Role-Based Access Control (RBAC): groups in Active Directory (AD) have been used to enforce role-based access controls. Users are assigned to groups based on their roles, which dictate their access to specific resources.
* Access Control Lists (ACLs): ACLs have been configured on AD objects, such as files, folders, and applications, to enforce permissions based on user group memberships.
* Group Policy Management: Group Policies have been applied to enforce security settings and restrictions on user workstations, limiting access to system resources based on user roles.
* Auditing: AD auditing has been enabled to monitor and log access to critical resources, ensuring compliance with access control policies.
* Least Privilege: Permissions have been assigned following the principle of least privilege, ensuring users have only the necessary access to perform their duties.
  + 1. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

**AC-5: Separation of Duties**

a. Identified and Documented Duties Requiring Separation

* Implementation:
  + Identification: Critical duties within the organization that require separation have been identified. These include roles such as system administrator, financial transaction initiator, approver, and auditor.
  + Documentation: These roles and the specific duties that need to be separated have been documented in the organization's access control policies. For example, financial transactions must be initiated by one individual and approved by another, ensuring that no single individual has both responsibilities.

b. Defined System Access Authorizations to Support Separation of Duties

* Implementation:
  + Role-Based Access Control (RBAC): Active Directory’s RBAC features have been used to create distinct security groups for each of the roles identified. For instance
    1. Employ the principle of least privilege, including for specific security functions and privileged accounts.

**AC-6: Least Privilege**

Implementation:

1. Role-Based Access Control (RBAC):
   * Users are assigned to AD security groups based on their job roles, granting only the minimum access rights needed to perform their tasks.
2. Access Control Lists (ACLs):
   * ACLs are configured on resources like files, folders, and applications to restrict access to only those AD groups or users who require it.
3. Privileged Account Management:
   * Privileged accounts are restricted to only necessary permissions, with administrative roles segmented to prevent excessive access.
4. Group Policy Management:
   * Group Policies enforce security settings, ensuring non-administrative users cannot access or modify system settings beyond their role’s requirements.
5. Review and Auditing:
   * Regular audits of user permissions and group memberships are conducted, with unnecessary privileges removed, and AD logs are monitored for unauthorized access attempts.

**3.1.6** Use non-privileged accounts or roles when accessing nonsecurity functions.

**Is satisfied with AC-6 Implementation**

* + 1. Monitor and control remote access sessions.

**AC-17: Remote Access**

Implementation:

* + Usage Restrictions:
    - Usage restrictions for remote access have been clearly defined and documented. Cisco AnyConnect has been configured to restrict access based on user roles and profiles, ensuring that only authorized roles can access specific resources remotely. Restrictions, such as prohibiting access from public Wi-Fi without using the VPN, are in place.
  + Configuration/Connection Requirements:
    - Cisco AnyConnect is configured to enforce endpoint security compliance before allowing connections. This includes ensuring that remote devices meet security criteria, such as having up-to-date antivirus software and an enabled firewall.
    - Multi-factor authentication (MFA) is enforced for all remote sessions through Cisco Duo, ensuring secure access.
    - All remote access connections use encrypted VPN tunnels to protect data in transit.
  + Implementation Guidance:
    - Comprehensive implementation guidance has been documented and distributed, covering installation, configuration, and usage of Cisco AnyConnect, along with security best practices and troubleshooting tips.

b. Authorized each type of remote access to the system prior to allowing such connections:

* Implementation:
  + Authorization Process:
    - A formal authorization process is in place for remote access. Each type of remote access has been reviewed and approved by IT security management before being enabled in Cisco AnyConnect. This process includes evaluating the necessity, risks, and required security controls.
  + Access Approval:
    - Remote access is only granted after the appropriate approvals have been obtained. The approval workflow involves sign-off from the user’s department head and the IT security team. Cisco AnyConnect profiles have been configured to enforce these access levels, with different profiles tailored to the specific needs of different user groups.
    1. Authorize remote execution of privileged commands and remote access to security-relevant information.

**AC-17(2): Protection of Confidentiality/Integrity Using Encryption**

Implementation:

* All remote access sessions through Cisco AnyConnect use encrypted VPN tunnels (TLS/IPsec) to protect the confidentiality and integrity of data in transit.
* Multi-factor authentication (MFA) via Cisco Duo is enforced for all remote sessions to ensure secure access.

**AC-17(3): Managed Access Control Points**

Implementation:

* Remote execution of privileged commands is restricted to authorized users through role-based access controls (RBAC) configured in Cisco AnyConnect.
* Privileged access is allowed only through designated VPN profiles and access points that are configured specifically for administrative roles.
* All privileged remote sessions are logged in detail.
  + 1. Verify and control/limit connections to and use of external systems.

**Implementation of AC-20: Use of External Systems**

Implementation:

* External System Verification:
  + All external systems connecting to the organization's network are required to pass security checks, including up-to-date antivirus, encryption, and compliance with security policies.
* Controlled Access:
  + External systems are only allowed to connect through a secure VPN with multi-factor authentication (MFA). Access is limited to specific resources based on role-based access controls (RBAC).
* Logging and Monitoring:
  + All connections from external systems are logged, and any unauthorized access attempts are monitored in real-time with alerts sent to the security team.

**Awareness and Training**

* + 1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

**AT-2: Awareness Training**

a. Provide security and privacy literacy training:

Initial and Ongoing Training:

All new users, including managers, senior executives, and contractors, receive mandatory security and privacy training during onboarding.

Refresher training is conducted annually for all users.

Training Updates:

Additional training is provided whenever there are significant system changes or after specific events such as security incidents or breaches.

b. Employ awareness techniques:

Awareness Techniques:

Regular phishing simulations are conducted to test and improve users' ability to recognize phishing attempts.

Monthly security newsletters are distributed, highlighting current threats and best practices.

Posters and digital signage around the workplace reinforce key security messages.

c. Update literacy training and awareness content:

Content Updates:

Training content is reviewed and updated annually to reflect new threats, technologies, and policies.

Immediate updates are made to training content following significant security incidents or changes in relevant laws or regulations.

d. Incorporate lessons learned from incidents:

Incident Integration:

Lessons learned from internal security incidents and breaches are incorporated into training materials and awareness campaigns.

Case studies of relevant external incidents are also used in training sessions to illustrate potential risks and preventive measures.

* + 1. **Ensure** that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

**AT-3: Role-Based Training**

Implementation:

a. Provide role-based security and privacy training:

* Targeted Roles and Responsibilities:
  + Training is provided to personnel with security-related roles, including system administrators, network engineers, security officers, and developers.
  + Initial and Ongoing Training:
    - Role-based training is conducted before personnel are authorized to access the system or perform their assigned duties.
    - Refresher training is provided annually to all personnel in these roles.
  + Training Updates for System Changes:
    - Additional training sessions are provided whenever there are significant system changes that affect how these roles interact with the system.

b. Update role-based training content:

* Content Update Frequency:
  + Role-based training content is reviewed and updated annually to reflect the latest threats, tools, and technologies relevant to each role.
  + Training content is also updated immediately following significant events such as security incidents or changes in regulations or organizational policies.

c. Incorporate lessons learned from incidents:

* Incident Integration:
  + Lessons learned from both internal and external security incidents are incorporated into role-based training. This includes case studies, analysis of what went wrong, and how similar incidents can be prevented in the future.

**Configuration Management**

* + 1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

**CM-2: Baseline Configuration**

Implementation:

a. Baseline Configuration Development and Maintenance:

* A baseline configuration for all network devices (router, firewall), workstations, and the Apache web server has been developed and documented. This includes hardware specifications, operating system versions, installed software, configuration settings, and network configurations.
* The baseline configuration is maintained under strict configuration control using a version-controlled configuration management tool. Any changes to the baseline are reviewed and approved before implementation.

b. Baseline Configuration Review and Update:

* Frequency: The baseline configuration is reviewed and updated annually.
* Trigger Events: The baseline is also updated whenever there is a significant change, such as the installation of new system components, upgrades, or patches.
* System Changes: Any installation or upgrade of system components, such as replacing or updating the router, firewall, workstations, or server, triggers an immediate review and update of the baseline configuration.
  + 1. Establish and enforce security configuration settings for information technology products employed in organizational systems.

**CM-6: Configuration Settings**

Implementation:

a. Establish and Document Configuration Settings:

* Configuration Baselines: Configuration settings for all components (router, firewall, workstations, and Apache web server) have been established and documented, reflecting the most restrictive mode consistent with operational requirements. These settings are based on [organization-defined common secure configurations], such as CIS Benchmarks or DISA STIGs.
* Secure Configurations:
  + Router: Access control lists (ACLs) and routing protocols are configured to limit exposure and access.
  + Firewall: Rules are configured to block all unnecessary inbound and outbound traffic, only allowing essential services.
  + Windows Workstations: Group Policies enforce strict security settings, including disabling unnecessary services, enforcing strong password policies, and limiting user privileges.
  + Apache Web Server: Configured with security modules (e.g., mod\_security) and hardened to minimize vulnerabilities, such as disabling directory browsing and ensuring all communications are encrypted.

b. Implement Configuration Settings:

* Deployment: The secure configuration settings have been implemented across all relevant components in the environment. Automated scripts and configuration management tools (e.g., Ansible, SCCM) are used to apply and verify these settings consistently across all devices.

c. Identify, Document, and Approve Deviations:

* Deviation Handling: Any deviations from the established configuration settings are identified and documented. Deviations are only allowed for [organization-defined system components], such as specific applications requiring less restrictive settings due to operational needs.
* Approval Process: All deviations are subject to an approval process based on [organization-defined operational requirements]. Justifications for deviations are reviewed and must be approved by the IT security team before implementation.

d. Monitor and Control Configuration Changes:

* Continuous Monitoring: Changes to configuration settings are monitored continuously using configuration management tools that track changes in real-time. Alerts are generated for any unauthorized or unexpected changes.
* Change Control Procedures: All changes to configuration settings are controlled in accordance with organizational policies. This includes logging changes, conducting regular audits, and ensuring that any modifications go through a formal change control process.

**Maintenance**

* + 1. Perform maintenance on organizational systems.

**MA-2: Controlled Maintenance**

Implementation:

a. Schedule, Document, and Review Maintenance:

* Scheduling: Maintenance, repair, and replacement activities for all system components are scheduled according to manufacturer/vendor specifications and organizational requirements.
* Documentation: Maintenance records are documented in a centralized maintenance management system, including details such as date, time, component serviced, actions taken, and personnel involved.
* Review: Maintenance records are reviewed quarterly by IT management to ensure compliance with maintenance schedules and standards.

b. Approve and Monitor Maintenance Activities:

* Approval: All maintenance activities, whether on-site or remote, must be approved by the IT department head or a designated security officer before they commence.
* Monitoring: On-site maintenance is supervised by authorized personnel, and remote maintenance is monitored in real-time using secure remote access tools. Logs of all maintenance activities are maintained and reviewed post-maintenance.

c. Approve Removal of System Components for Off-Site Maintenance:

* Approval Process: The removal of any system or system components from organizational facilities for off-site maintenance, repair, or replacement must be explicitly approved by the Chief Information Officer (CIO) or their delegate.

d. Sanitize Equipment Before Off-Site Maintenance:

* Sanitization Procedure: Before any equipment is removed for off-site maintenance, all associated media must be sanitized to remove [organization-defined sensitive information, such as Personally Identifiable Information (PII), company proprietary data, and sensitive configuration files]. Sanitization is performed in accordance with NIST SP 800-88 guidelines.
* Verification: The sanitization process is verified by a second individual to ensure all data is properly removed before the equipment leaves the facility.

e. Verify Control Functionality Post-Maintenance:

* Post-Maintenance Check: After maintenance, repair, or replacement activities, all potentially impacted security controls (e.g., firewall configurations, access control settings) are checked to ensure they are still functioning correctly. This includes testing any related systems to confirm they operate as expected.

f. Include Required Information in Maintenance Records:

* Maintenance Records Content: Organizational maintenance records include the following information:
  + Date and time of maintenance
  + Description of the maintenance activity
  + Identification of the system/component serviced
  + Name of the technician(s) performing the maintenance
  + Approval details for the maintenance activity
  + Any deviations from standard procedures and justifications
  + Results of post-maintenance control checks
  + Sanitization certification (if applicable)
    1. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

**MA-3: Maintenance Tools**

Implementation:

a. Approve, Control, and Monitor the Use of System Maintenance Tools:

* Tool Approval: All system maintenance tools, including hardware and software, must be approved by the IT Security Manager before use. This includes both general-purpose tools and specialized tools specific to the environment.
* Tool Inventory: An inventory of all approved maintenance tools is maintained in a centralized database, including tool names, versions, and associated vendors.
* Access Control: Only authorized personnel, as identified by their roles and responsibilities, are granted access to these tools. Access permissions are managed through role-based access controls (RBAC) in the organization’s identity management system.
* Monitoring: The use of maintenance tools is monitored in real-time. Logging mechanisms are in place to record all maintenance activities, including which tools were used, by whom, and when. These logs are regularly reviewed by the IT security team.

b. Review Previously Approved System Maintenance Tools:

* Review Frequency: All approved system maintenance tools are reviewed semi-annually to ensure they remain necessary, effective, and secure.
* Review Process: The IT Security Manager leads the review process, which includes evaluating the tool’s performance, checking for updates or vulnerabilities, and ensuring continued alignment with organizational security policies.
* Decommissioning: Tools that are no longer deemed secure or necessary are decommissioned and removed from the inventory, with access permissions revoked.
  + 1. Ensure equipment removed for off-site maintenance is sanitized of any CUI.

**MA-5: Maintenance Personnel**

Implementation:

a. Establish a Process for Maintenance Personnel Authorization:

* Authorization Process: A formal process has been established for authorizing maintenance personnel who will perform maintenance on organizational systems. This process includes background checks, verification of qualifications, and security clearance checks.
* Authorized Personnel List: A list of authorized maintenance personnel and organizations is maintained in a secure, centralized database. This list is regularly updated and includes details such as names, roles, access levels, and expiration of authorizations.

b. Verify Access Authorizations for Non-Escorted Personnel:

* Verification Process: Non-escorted personnel performing maintenance on systems are required to have their access authorizations verified before starting any work. Verification includes checking against the authorized personnel list and ensuring that their clearance level is appropriate for the work they will be performing.
* Access Controls: Only personnel with verified and appropriate access authorizations are allowed to work unescorted. This process is enforced by security staff or designated IT personnel.

c. Designate Personnel to Supervise Non-Authorized Maintenance Activities:

* Designation of Supervisors: Organizational personnel with the required access authorizations and technical competence are designated to supervise maintenance activities performed by personnel who do not possess the required access authorizations.
* Supervision Protocol: Supervisors are responsible for overseeing all activities, ensuring that non-authorized personnel do not access sensitive areas or data. The supervisor must be present throughout the maintenance process and must document all activities performed by non-authorized personnel.

**Physical Protection**

* + 1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

**PE-2: Physical Access Authorizations**

Implementation:

a. Develop, Approve, and Maintain a List of Authorized Individuals:

* Access List Creation: A list of individuals with authorized access to the facility where the system resides has been developed and approved by the security management team.
* Maintenance: This list is maintained in a secure, centralized access control system. The list includes details such as names, roles, access levels, and the areas within the facility they are authorized to access.

b. Issue Authorization Credentials:

* Credentials Issuance: Authorized individuals are issued access credentials, such as key cards or biometric access profiles, that grant entry to specific areas within the facility. These credentials are linked to the individual’s role and level of authorization.
* Access Control Integration: The credentials are integrated with the facility’s physical access control system, ensuring that only those with proper authorization can enter secured areas.

c. Review the Access List:

* Review Frequency: The access list is reviewed quarterly by the security management team to ensure it remains accurate and up-to-date.
* Review Process: The review involves verifying that only individuals with a current need for access are on the list and that their access levels are appropriate for their roles.

d. Remove Individuals from the Access List:

* Removal Process: Individuals are promptly removed from the facility access list when they no longer require access, such as when they change roles, leave the organization, or their access authorization is revoked.
* Deactivation: Their access credentials are immediately deactivated in the access control system to prevent unauthorized access.
  + 1. Protect and monitor the physical facility and support infrastructure for organizational systems.

**PE-6: Monitoring Physical Access**

Implementation:

a. Monitor Physical Access:

* Surveillance Systems: Closed-circuit television (CCTV) cameras are installed at all entry points, sensitive areas, and around the perimeter of the facility where the system resides. These cameras provide continuous monitoring and are configured to trigger alerts on detecting unauthorized access or suspicious activities.
* Access Control Logs: Physical access to the facility is monitored through an electronic access control system that logs every entry and exit. Alerts are generated for any unauthorized access attempts or forced entry events.
* Security Personnel: On-site security personnel continuously monitor the live feed from CCTV cameras and respond to any physical security incidents as they occur.

b. Review Physical Access Logs:

* Review Frequency: Physical access logs are reviewed weekly by the security management team to ensure that only authorized personnel are accessing the facility.
* Event-Triggered Review: In addition to regular reviews, the logs are reviewed immediately following any suspicious events, such as unauthorized access attempts, alarms triggered by the access control system, or reports of lost or stolen access credentials.
* Detailed Analysis: The review includes analyzing access patterns, identifying anomalies, and verifying that all access events correspond to legitimate activities.

c. Coordinate with Incident Response Capability:

* Incident Response Coordination: Any suspicious findings or confirmed physical security incidents identified during the review of access logs are immediately reported to the organizational incident response team.
* Joint Investigations: The security management team coordinates with the incident response team to investigate physical security incidents, correlating physical access data with other incident data to determine the scope and impact.
* Post-Incident Review: After an incident is resolved, a joint post-incident review is conducted to assess the effectiveness of the physical security measures and to update procedures as necessary.
  + 1. Escort visitors and monitor visitor activity.

**PE-8: Visitor Access Records**

Implementation:

a. Maintain Visitor Access Records:

* Record-Keeping: Visitor access records are maintained for a period of one year. These records include the visitor’s name, organization, purpose of visit, entry and exit times, the area(s) accessed, and the name of the escort.
* Secure Storage: All visitor access records are securely stored in an electronic access control system, which is backed up regularly to ensure data integrity and availability.

b. Review Visitor Access Records:

* Review Frequency: Visitor access records are reviewed on a [organization-defined frequency, e.g., monthly] basis by the security management team to ensure compliance with visitor policies and to detect any unusual patterns or anomalies.
* Review Process: During the review, the team checks for completeness of records, adherence to escort policies, and any irregularities, such as repeated visits by the same individual without a clear business reason.

c. Report Anomalies:

* Anomaly Reporting: Any anomalies or suspicious activities identified during the review of visitor access records are promptly reported to [organization-defined personnel, e.g., the Chief Security Officer (CSO) or the Incident Response Team]. This may include unexplained access to sensitive areas, discrepancies in entry/exit times, or visitors who were not properly escorted.
* Incident Response Coordination: The reported anomalies are investigated in coordination with the organizational incident response team, and appropriate actions are taken based on the findings.
  + 1. **Control and manage physical access devices.**

**Implementation:**

a. Enforce Physical Access Authorizations:

* Entry and Exit Points: Physical access authorizations are enforced at [organization-defined entry and exit points, e.g., main entrance, server room entrance] of the facility where the system resides.
  1. Verification: Individual access authorizations are verified before granting access to the facility using electronic access control systems, which include card readers and biometric scanners.
  2. Ingress and Egress Control: Ingress and egress to the facility are controlled using electronic key card systems, biometric readers, and security guards.

b. Maintain Physical Access Audit Logs:

* Audit Logs: Physical access audit logs are maintained for all [organization-defined entry or exit points, e.g., all entrances to the data center] and stored securely in the access control management system.
* Log Retention: These logs are retained for [organization-defined time period, e.g., one year] and are reviewed regularly to detect any unauthorized access attempts.

c. Control Access to Publicly Accessible Areas:

* Public Access Control: Areas within the facility designated as publicly accessible, such as lobbies or reception areas, are controlled using visitor registration systems, security cameras, and physical barriers.
* Restricted Access: Access to secure areas beyond the publicly accessible zones is restricted to authorized personnel only.

d. Escort Visitors and Control Visitor Activity:

* Visitor Escorts: Visitors are escorted by authorized personnel at all times in [organization-defined circumstances, e.g., when accessing sensitive areas such as server rooms].
* Activity Monitoring: Visitor activity is monitored continuously during their stay, and their access is limited to the areas necessary for their visit.

e. Secure Keys, Combinations, and Other Physical Access Devices:

* Device Security: All physical access devices, including keys and combination codes, are stored securely in a locked, restricted-access area when not in use.
* Access Control: Only authorized personnel have access to these physical access devices.

f. Inventory Physical Access Devices:

* Inventory Management: An inventory of keys, access cards, and combination locks is conducted every quarter. The inventory is documented, and any discrepancies are investigated immediately.

g. Change Combinations and Keys:

* Key/Combination Changes: Combinations and keys are changed every annually or immediately when keys are lost, combinations are compromised, or when personnel possessing the keys or combinations are transferred or terminated.

**System and Communications Protection**

**3.13.2** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

**SC-2: Application Partitioning**

Implementation:

1. User and Management Interface Segregation:
   * Separate Systems: User functionality and system management functionality are hosted on separate systems or logical partitions within the environment. For example, the user-facing web application is hosted on a dedicated server, while the management console is hosted on a separate, restricted server.
   * Network Segmentation: The network is segmented to separate user traffic from management traffic. VLANs or separate subnets are used to ensure that management interfaces are not accessible from the user network.
   * Access Control: Access to system management functions is restricted to authorized administrators only. Role-based access controls (RBAC) are implemented to enforce this separation, ensuring that regular users do not have access to system management interfaces.
2. Dedicated Management Interfaces:
   * Separate Login Portals: Management interfaces are accessible only through dedicated login portals that are separate from the user interface. These management portals are protected by multi-factor authentication (MFA) and strong password policies.
   * Restricted Access Points: Management interfaces are only accessible from specific, secured workstations or via a secure VPN connection, ensuring that only authorized personnel can access these functions.
3. Software Architecture:
   * Logical Separation: The software architecture is designed to logically separate user processes from management processes. For example, user sessions are handled by separate application modules or services that do not have direct access to system management functions.
   * APIs and Service Interfaces: APIs or service interfaces that support system management functions are not exposed to end-users. These interfaces are only accessible by system administrators through secure, authenticated connections.
4. Monitoring and Auditing:
   * Activity Logging: All access to system management functions is logged and monitored. Logs are stored securely and reviewed regularly to detect any unauthorized access attempts or anomalies.
   * Audit Controls: Regular audits are conducted to ensure that the separation of user and management functionality is maintained and that no unauthorized cross-access occurs.

**System and Information Integrity**

**3.14.1** Identify, report, and correct system flaws in a timely manner.

**SI-2: Flaw Remediation**

Implementation:

a. Identify, Report, and Correct System Flaws:

* Vulnerability Scanning: Regular automated vulnerability scans are conducted across all systems to identify potential flaws in software, firmware, and configurations.
* Reporting Process: Identified flaws are documented and reported immediately to the IT security team. A centralized ticketing system is used to track the status of each flaw, from identification to remediation.
* Corrective Actions: Flaws are prioritized based on severity and potential impact. Critical flaws are corrected immediately, while lower-priority flaws are addressed according to the organization's risk management plan.

b. Test Software and Firmware Updates:

* Testing Environment: All software and firmware updates related to flaw remediation are first tested in a controlled, isolated environment that mirrors the production system. This testing is done to verify the effectiveness of the update and to identify any potential side effects.
* Evaluation: The updates are evaluated for compatibility with existing systems, ensuring that they do not introduce new vulnerabilities or disrupt normal operations.
* Approval: Only after successful testing and approval by the IT security team are the updates scheduled for deployment in the production environment.

c. Install Security-Relevant Updates:

* Time Period for Installation: Security-relevant software and firmware updates are installed within [organization-defined time period, e.g., 30 days] of their release. For critical updates, a shorter time frame (e.g., within 48 hours) is enforced.
* Patch Management System: A patch management system is used to automate the deployment of updates across all systems, ensuring timely and consistent application of patches.

d. Incorporate Flaw Remediation into Configuration Management:

* Configuration Management Integration: The flaw remediation process is integrated into the organizational configuration management process. This includes:
  + Baseline Updates: Updating baseline configurations to reflect the applied patches and updates.
  + Documentation: Documenting all changes made during flaw remediation in the configuration management database (CMDB).
  + Version Control: Maintaining version control over all system components to track changes resulting from flaw remediation efforts.
  + Change Control: All flaw remediation activities follow the organization's change control procedures, including obtaining necessary approvals before making changes to the production environment.