**Complete implementation details for the control listed below using NIST SP800-53 RV 5. Please submit by Thursday June 6, 2024.**

|  |  |  |
| --- | --- | --- |
| **AC-6** | | **LEAST PRIVILEGE** |
| **Control Requirement:**  Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks. | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:** Only System Administrators and designees are allowed to access system. | | |

|  |  |  |
| --- | --- | --- |
| **AC-6 (1)** | | **LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS** |
| **Control Requirement:**  Prohibit privileged access to the system by non-organizational users. | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:**  Use firewalls, VLANs, and other network controls to enforce these boundaries.  Also Ensure that only authorized personnel can obtain privileged accounts. | | |

|  |  |  |
| --- | --- | --- |
| **CM-02** | | **BASELINE CONFIGURATION** |
| **Control Requirement:**   1. Develop, document, and maintain under configuration control, a current baseline configuration of the system; 2. Review and update the baseline configuration of the system: 3. [Assignment: organization-defined frequency]; 4. When required due to [Assignment: organization-defined circumstances];   3. When system components are installed or upgraded | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:**   1. **Identify the Systems**: Determine which systems, applications, and components are within the scope for baseline configuration. **Inventory**: Create a detailed inventory of hardware, software, and network configurations for each system. Include versions, patch levels, and settings. **Configuration Management Database (CMDB):** Use a CMDB to store and manage configuration items and their relationships. Ensure it is kept up to date with the latest configuration information. **Automate Deployment:** Use configuration management tools like Ansible, Puppet, or Chef to automate the deployment and enforcement of baseline configurations **Monitoring and Reporting:** Implement continuous monitoring of systems to detect deviations from the baseline configuration. Use tools like Tripwire or SCCM (System Center Configuration Manager) for this purpose. 2. 1. **Risk Assessment:** Conduct a risk assessment to determine the appropriate review frequency. Consider factors such as the system's criticality, sensitivity of the data, and the threat landscape. 2. **Monitor Changes:** Continuously monitor the system for any changes that may impact the baseline configuration, such as software updates, patches, or configuration drift. 3. **Utilize Configuration Management Tools:** Implement automated configuration management tools such as Puppet, Chef, or Microsoft System Center Configuration Manager (SCCM) to manage and enforce baseline configurations across the system | | |

|  |  |  |
| --- | --- | --- |
| **RA-05** | | **Vulnerability Scanning and Remediation** |
| **Control Requirement:**  The organization scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or in response to organization-defined events] and when new vulnerabilities potentially affecting the system/applications are identified and reported. The organization remediates vulnerabilities in accordance with an organizational assessment of risk. | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:** The organization should conduct vulnerability scans at regular intervals based on risk assessment, organizational policies, and regulatory requirements | | |

|  |  |  |
| --- | --- | --- |
| **MA-05** | | **Security Training** |
| **Control Requirement:**  organizations to provide security training to personnel commensurate with their assigned roles and responsibilities. | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:** Organizations should develop a comprehensive security training program that covers various topics, including phishing awareness, password security, data protection, incident reporting procedures, and compliance requirements. | | |

|  |  |  |
| --- | --- | --- |
| **PE-15** | | **Cryptographic Protections** |
| **Control Requirement:**  organizations to employ cryptographic mechanisms to protect the confidentiality and integrity of personally identifiable information (PII) and other sensitive information in accordance with applicable laws, regulations, and policies. | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:** Organizations implementing PE-15 should consider employing encryption, digital signatures, and other cryptographic techniques to safeguard sensitive data. Additionally, compliance with relevant cryptographic standards (e.g., FIPS 140-2) may be necessary depending on the context and regulatory requirements. | | |

|  |  |  |
| --- | --- | --- |
| **SA-3** | | **Security Assessment Organizational Assessment** |
| **Control Requirement:**  assess security controls' effectiveness, and ensure compliance with security policies and standards. | | |
| **Implementation Status**   * Implemented * Not Implemented * Planned * Not Applicable |  | |
| **Control Type:** | **Common Control** | |
| **Implementation Details:** Organizations are expected to implement SA-3 by establishing and maintaining processes for conducting security assessments at regular intervals. This may involve defining assessment methodologies, scheduling assessments, assigning responsibilities, conducting assessments, analyzing results, and taking corrective actions as necessary. | | |