**1. Can you describe the organization’s approach to implementing the principle of least privilege? AC-6 (1) *"Least Privilege – Authorize Access to Security Functions" – Restrict Privilege***

* **Response:** Our approach involves assigning users the minimum level of access required to perform their job functions. We regularly review and adjust access permissions based on role changes and ensure that access is restricted to the least necessary privileges.

**2. How does the organization define and manage user roles and permissions? AC-6 (2) *"Least Privilege –*** ***Non-privileged Access for Nonsecurity Functions” - Role-Based Access Control***

* **Response:** We define user roles based on job functions and responsibilities. Permissions are granted according to these predefined roles, and access rights are managed through our identity and access management system. We conduct periodic role reviews to ensure accuracy.

**3. What processes are in place to ensure that privileged accounts are properly managed? AC-6 (3) *"Least Privilege – Network Access to Privileged Commands” - Privileged Access Management***

* **Response:** Privileged accounts are managed with multi-factor authentication, but the review process is not as frequent as it should be. We perform audits annually, whereas more frequent reviews are recommended.

**4. How does the organization handle temporary or emergency access requests? AC-6 (4) *"Least Privilege – Separate Processing Domains” - Temporary Elevation of Privileges***

* **Response:** For temporary or emergency access, we follow a formal request process that includes management approval. Temporary access is granted only for the required duration and is automatically revoked after the specified time. We log all such requests for auditing purposes.

**5. Can you describe how user access reviews and audits are conducted? AC-6 (5) *"Least Privilege – Privileged Accounts” - Periodic Review of Privileges***

* **Response:** " Access reviews are done semi-annually, and while we do compare permissions to job roles, the process is sometimes delayed. Audit logs are reviewed, but not on a consistent basis."

**6. How does the organization ensure that contractors or third-party vendors adhere to the principle of least privilege? AC-6 (6) *"Least Privilege – Privileged Access by Non-organizational Users” - Contractor and Third-Party Access***

* **Response:** "Contractors and third-party vendors are granted access only to the systems and data necessary for their work. We use separate accounts for external parties with restricted permissions and require them to comply with our security policies. Their access is monitored and reviewed periodically."

**7. Are there any automated tools or systems used to manage and enforce least privilege policies? AC-6 (7) *"Least Privilege – Review of User Privileges” - Automated Tools***

* **Response:** "Yes, we use an identity and access management (IAM) system that automates the process of assigning and revoking permissions. This tool helps enforce least privilege by providing role-based access control (RBAC) and auditing capabilities."

**8. What steps are taken to ensure that least privilege principles are applied to system configurations and applications? AC-6 (8) *"Least Privilege – Privilege Levels for Code Execution” - System and Application Configuration***

* **Response:** "Least privilege principles are generally applied to system configurations, but we occasionally face challenges with legacy systems that may have broader permissions than required. We are working on addressing these issues."

**9. How is compliance with the least privilege control verified and validated? AC-6 (9) *"Least Privilege – Log Use of Privileged Functions” - Verification and Validation***

* **Response:** "Compliance is verified through regular internal audits, including reviews of access controls and permissions. We also conduct vulnerability assessments and penetration tests to ensure that least privilege principles are effectively enforced."

**10. Can you provide examples of any recent changes or improvements made to enhance least privilege controls? AC-6 (10) *"Least Privilege – Prohibit Non-privileged Users from Executing Privileged Functions” - Continuous Improvement***

* **Response:** "Recently, we implemented automated tools for managing permissions more effectively and introduced periodic role reviews to ensure that access remains appropriate. We also updated our policies to include more stringent controls for privileged accounts."