**1. Project Overview**

- **Objective:**
    - To define, test, and document the process of encrypting restricted data, backing up the data to the cloud, and successfully recovering the data on a new server.
    - The PoC involves sensitive data, requiring US-based freelancers with strong technical writing and documentation skills.

**2. Scope of Work**

- **Encryption:**
    - Folders containing restricted data that need to be encrypted will already be identified.
    - The data to be encrypted will be no more than 10 GB of test data.
    - Encrypt both application data and the associated database, which reside on the server.
    - EFS encryption (AES-256) should be used to encrypt the identified data.
    - Encryption certificates may need to be installed on workstations if required to access encrypted data on the server.
- **Backup:**
    - Backup the encrypted data to a designated cloud storage solution (Synology C2 Backup for Business).
    - Ensure that the backup process can be automated and tested periodically for successful completion.
    - Confirm the integrity of the encrypted data after it is uploaded to the cloud.
- **Recovery:**
    - Simulate a disaster recovery scenario where a new server is provisioned.
    - Retrieve the encrypted data from the cloud backup and restore it on the new server.

    - Test the successful decryption of data and ensure that the application and client software can access and function with the restored data.

- **Documentation:**
    - Create detailed documentation outlining the entire process, including steps for encryption, backup, and recovery.
    - The documentation should include:
        1. Software and tools used
        2. Configuration details
        3. Encryption keys management
        4. Step-by-step recovery instructions
        5. Testing results
        6. Troubleshooting tips for potential issues during recovery

**3. Technology Requirements**

- **Server Environment:**
    - A basic Azure Lab environment is in place with a Windows 2019 Server and a Windows 11 Workstation.  Further configuration may be required.
    - Information only:  In the real production environment, the application resides on a server connected to a small network of workstations, with corresponding client software accessing the application data.
    - The environment may include Windows Server for hosting the application and workstations running Windows OS.
- **Cloud Backup Solution:**
    - The cloud backup solution is Synology C2 Backup for Business.
- **Encryption Tools:**
    - Windows EFS or third-party encryption software.

**4. Testing Criteria**

- **Encryption:**

    - Data must be successfully encrypted without disrupting the operation of the application.
- **Backup:**
    - Backup integrity must be verified post-encryption.
    - Test backup schedules and automation to ensure periodic backups without data corruption.
- **Recovery:**
    - Data must be restored on a new server from the cloud, with successful decryption.
    - The restored data should be accessible and usable by the application without data loss or application issues.

**5. Deliverables**

- **Fully Documented Process:**
    - Detailed documentation of the encryption, backup, and recovery processes.
    - A finalized version of the documentation should include configuration steps, screenshots, software versions, and any relevant testing logs or results.
- **Test Report:**
    - Provide a report summarizing the PoC results, including any issues encountered during the encryption, backup, and recovery processes and how they were resolved.
- **Technical Writing Quality:**
    - Documentation must be clear, concise, and suitable for a technical audience who may need to replicate the process.
    - The freelancer should provide high-quality technical writing skills and demonstrate an ability to document technical procedures accurately.

**6. Freelancer Qualifications**

- **Technical Skills:**
    - Experience in server management, encryption, cloud backup, and recovery processes.

    - Familiarity with tools such as Windows Server, cloud storage providers (e.g., AWS, Azure), and encryption software.
- **Documentation Skills:**
    - Proven experience in technical writing and creating clear, detailed, and organized documentation for technical processes.

**7. Timeline and Milestones**

- **Milestone 1:** Encrypt the data and document the encryption process.
- **Milestone 2:** Set up and test the cloud backup process.
- **Milestone 3:** Simulate the disaster recovery and restore the data on a new server.
- **Milestone 4:** Provide final documentation and testing report for review.