Cloud Computing Use Statement

Principal Investigator (PI): ___________________________________

Institution: University of Washington

Cloud Service Provider (CSP): Microsoft Government Community Cloud High

Description of Cloud Services:

1. **Type of Service:**
   - Platform as a Service (PaaS)
2. **Purpose of Use:**

3. **Security Measures:**
   - The cloud environment is configured to align with NIST SP 800-171 standards, ensuring the protection of Controlled Unclassified Information (CUI). Security measures include:
     - **Access Control:** Implementing multi-factor authentication (MFA) and role-based access controls to ensure only authorized personnel can access sensitive data.
     - **Audit and Accountability:** Maintaining detailed logs of all access and activities within the cloud environment to monitor and respond to any unauthorized access or anomalies.
     - **Configuration Management:** Regularly updating and patching systems to protect against vulnerabilities and ensuring configurations are compliant with security policies.

        - **Incident Response:** Establishing a comprehensive incident response plan to quickly address and mitigate any security incidents.
        - **Media Protection:** Ensuring that all media containing sensitive data is properly encrypted and securely disposed of when no longer needed.
        - **System and Communications Protection:** Utilizing encryption for data in transit and at rest to protect against unauthorized access and data breaches.
        - **System and Information Integrity:** Regularly monitoring and scanning systems for vulnerabilities and implementing measures to protect against malware and other threats.

4. **Data Management Plan:**
    - Data will be managed in accordance with NIH GDS Policy, NIH Security Best Practices for Controlled-Access Data, and NIST SP 800-171 standards, including:
        - **Access Controls:** Implementing strict access controls to ensure that only authorized personnel can access sensitive data.
        - **Data Backup:** Regularly backing up data to ensure its availability and integrity in case of data loss or corruption.
        - **Data Encryption:** Encrypting data both in transit and at rest to protect against unauthorized access and data breaches.
        - **Data Retention:** Implementing data retention policies to ensure that data is retained for the required period and securely disposed of when no longer needed.
5. **Compliance:**
    - The institution and CSP comply with NIH GDS Policy, NIH Security Best Practices for Controlled-Access Data, and NIST SP 800-171 standards. This includes:
        - **Institutional Compliance:** Ensuring that the institution's management of the GCC High environment is compliant with NIST SP 800-171 standards.
        - **Third-Party Compliance:** Verifying that any third-party cloud service providers facilitating operational support and/or used for data storage and analysis are compliant with NIST SP 800-171 standards.

- **Attestation:** Providing NIH with an attestation affirming that the institution and CSP comply with relevant NIH policies and standards.

Request for Permission:

The PI formally requests permission to use the Microsoft Government Community Cloud High environment as their cloud service provider for the storage and analysis of data. This request is made in accordance with NIH guidelines and standards, ensuring that all data will be managed and protected in compliance with NIH Security Best Practices for Controlled-Access Data and NIST SP 800-171 standards.

Approval and Attestation:

By submitting this request, the Principal Investigator attests that the information provided in this Cloud Computing Use Statement is accurate and that the institution and CSP comply with relevant NIH policies and standards.