<u>Subject: -</u> Service contract for **“Digital Library Power Plant”.**

<u>SCOPE OF Work –</u>

1.Set up an online platform for management of all documents, drawings, reports etc. of CLIENT Power-1740MW. The system upload and download speed should be very fast for large files too.

2.The digital platform will provide indexing, categorization, sizing, zipping, downloading, and uploading features.

3.The document once uploaded will not be deleted but can be revised, discarded or no longer use documents will be termed as obsolete and categorized accordingly.

4.The online portal will include features of the version management system.

5.The document will be aligned with documentation protocols for audit purposes such as IMS, ISO, etc.

6.The service provider will also provide a comprehensive online platform with the mentioned features. (subject to change only after technical discussion)

a.Analysis dashboard for usage and its

b.Integration with Microsoft Azure.

7. Dashboard must be in line with Client’s cybersecurity standards, providing AD-ID logins.

8. The digital library will consist of documents in all the format not limited to .pdf/.dwg/.stl/.dwf/.jpg/.jpeg/.png etc.

9. PARTNER will also make sure that Client has direct access to its teams (local or international) who will be engaged in this project from design to deployment.

10. This Application/ Solution shall be secured from any virus, malwares, hacking and spams etc.

11. Access to Application shall be through secured authentication mechanism as per CLIENT IT Security policy.

12. Data exchange should abide by all laws on privacy and data protection Security Architecture. The proposed solution shall adhere to the guidelines & frameworks issued by CLIENT IT policy.

13. The basic tenets of CLIENT security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders.

14. Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.

15. Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the Databases.

16. Maintaining Date/Time Stamp and User Id: Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.

17. Audit trails or audit logs should be maintained. Log information is critical in identifying and tracking threats and compromises to the environment.

18. A strong authentication mechanism should be considered to protect unauthorized access to the CLIENT applications as per CLIENT policy.

19. Secure coding guidelines should be followed. Secure coding guidelines should include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard should be mapped in the secure coding guidelines to cover all major vulnerabilities.

20.Establish processes for viewing logs and alerts which are critical to identify and track threats and compromises to the environment. The granularity and level of logging must be configured to meet the security management requirements.

21.User shall be able to define multiple email ids where daily reports can be auto sent at configurable time.

22.Application shall be integrated to Client Active directory server for SSO.

23.System shall have provision for blocking/unblocking users.

24.System shall support testing of processes and workflows defined with test data before making it live.

25.Predefined templates to be made available for ease of configuration and faster integration.

26.PARTNER needs to implement suitable PIP in the project.

27.Every process and procedure implemented in this project must be reviewed and updated by PARTNER at least on an annual basis from the Go-Live Date.

28. Regular auditing is an inspection or examination of infrastructure to evaluate or improve its appropriateness, safety and efficiency.

29. The portal will provide cloud-based storage integrated with Client Microsoft Azure platform.

30. Front end of Digital platform will be based upon Library and segmentation picturizations to enable interactive user interface.

31. PARTNER is responsible for maintaining the data privacy of the systems used and solution deployed.

32. PARTNER shall ensure that the client solution details and transactions should not be passed to other clients.

33. PARTNER shall ensure that the saved user data should be encrypted and should be accessed by authorized personnel using secured user credentials.

34.PARTNER is responsible for preparing the DR plan, to sustain entire system if primary setup goes down or doesn’t work.

35.PARTNER shall ensure that the solution should have proper data backup for sustaining the solution and historical data.