Draft Requirements for Data Centralisation and Security

Brief:

Directorate General of Hydrocarbons (Under Ministry of Petroleum & Natural Gas, Govt. of India) intends to implement a comprehensive IT solution including centralized storage of critical data, with regular backups aligned with industry best practices and mechanisms to secure sensitive information on end-user devices.

Proposed Solution:

The comprehensive solution will consist of three key components to achieve the desired objectives:

Centralized Network Attached Storage (NAS): To provide a storage system for critical data, ensuring easy access, management, and scalability across the organization.

Backup Storage and Software: To regularly back up data according to industry best practices, ensuring data integrity, availability, and quick recovery in case of data loss or system failures.

Data Loss Prevention (DLP) Solution: To safeguard sensitive information by monitoring, detecting, and preventing unauthorized access, transmission, or leakage of data, both within and outside the organization.

The features/specifications of each component are broadly listed below

1. ***Primary NAS Storage***:

Parameter	Specification
Architecture	- Offered product shall be scale-out file storage supporting NFS and SMB natively - Offered Storage platform shall be all NVMe SSD disk-based architecture.
Capacity & Scalability	- Storage shall be configured with 100 TB of Usable capacity. - Storage shall be scalable to 200 TB of Usable capacity in the same single unified addressable name space.
Controllers	- Storage should have minimum 2 controllers configured in active-active configuration with No Single Point of Failure architecture. - Storage should have minimum 64 GB Memory installed per controller.
WORM Support	Storage shall include capability with required licenses for protecting files from modification or deletion until a specified retention date to allow creation of permanent, unalterable set of files and directories and ensure the integrity of data. The requested functionalities must be configurable from the GUI/Web Interface for the administrators.
Storage Efficiency	Storage shall be offered with both in-line de-duplication and compression functionality.
Protocol Support	Storage should be bundled with NFS, CIFS (SMB), FTP, FC and iSCSI protocols.
Resiliency and High Availability	Controllers/Nodes must have redundant back plane connectivity / cluster interconnects, to ensure that there is no Single Point of Failure (SPOF). Storage should support Non-disruptive maintenance, upgrade, and scale-out clustering
Front-end - Client connectivity Layer	Each front-end controller shall also be offered with 2 x 10Gbps Ethernet Front-end ports.

2. ***Backup Solution:***

Specification
The solution should be proposed with 50TB capacity on appliance along with upfront backup software capacity license for 50TB.
Proposed backup appliance should support industry leading backup software and should support deduplication at backup server/ host / application level.

Offered disk-based backup device must support encryption functionality.
Backup software must have the ability to perform cross hardware restore with different hardware configurations.
The proposed solution should have a mechanism to perform automatic data integrity check on the backup data to ensure the data integrity without the need of any additional third-party software
The backup software should support creation of different schedules and policies for creating backups and their retention.
Comprehensive reporting of media, backup server, jobs, analytics should be offered as part of the functionality in the supplied software.

3. End Point DLP Solution:

Specification
Solution should be able to identify Sensitive Data using Sensitive Keyword based markers, Pattern/Regex based markers, Unstructured Fingerprinted Data based markers, file attributes-based markers
Solution should be able to block data transfer via devices (USB drives, MTP, Printers, CD/DVD, Bluetooth Connected devices etc) and prevent Data Loss via devices (USB drives, Printers) using content identification
Solution should be able to prevent Data Loss via enforced encryption of USB storage devices and identify and whitelist USB storage devices for internal use
Solution should be able to Block Web File Uploads based on Whitelisted or Blacklisted Domains or Email Addresses (Sender domain), File Type, File Attributes (Password Protection / Data Classification Meta Tags) and File Names while also sensitive content inside files
Solution should be password protected from being uninstalled and should be tamper proof.
Solution should support integrations with Microsoft Active Directory; for scheduled Sync of organization and User information
Proposed Solution should be capable of providing options for Customised Pop-up Messages for any blocked activity.
Solution should allow enforcement of Single DLP policy enforcement across web, email, cloud, endpoint, egress channels.
Solution should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint
Solution should have the ability to identify User malicious activities and behavioural anomalies across channels
Solution should be able to implement temporary policies for uplifting the user privileges for a defined duration
License must be provided for 300 Machines/Users for 5 years

Scope of Work:

The deployment of the comprehensive IT solution must be completed in three phases:

Phase 1: User Onboarding and Directory Setup

- Onboard users to Microsoft Active Directory platform
- Create hierarchical segregation of users based on departments and functional reporting.

Phase 2: Storage and Backup Deployment

- Deploy and configure NAS storage in DGH premises
- Allocate storage pools and enable auto-availability of mapped directories to respective desktop PCs through AD.
- Create AD policies to ensure sync to data from desktop PC to NAS
- Deploy and configure backup solution to ensure redundancy and data availability

Phase 3: DLP Solution Deployment

- Install and configure DLP solution on end-user desktops as per policies

Additional Points:

1. Warranty period for all hardware components must be **3 years** followed by **AMC period** of **2 years**
2. Solution proposed must include all the required hardware & software keeping the above requirements/specifications in consideration which may also include any additional components necessary to make the system functional.
3. OEM Rack must be included with hardware requiring rack-based installation.
4. Other requirements like power, cooling and internet bandwidth and connectivity will be provided by DGH
5. Budgetary Quotations must include applicable taxes.