دولـة الكــــويت

المؤسسة العامة للرعاية السكنية

المـؤسسـة العـامـة للـرعـايـة السكنيـة
Public Authority for Housing Welfare

REQUEST FOR PROPOSAL

كراسة المواصفات الفنية الخاصة بمناقصة
تهيئة بيئة النسخ الاحتياطي بالمؤسسة العامة للرعاية السكنية
2025

Table of Contents

1. Introduction

The Public Authority for Housing Welfare (PAHW) is a leading governmental organization located in the south of Surah (ministries zone) responsible for the planning, designing, and execution of housing programs for Kuwaiti citizens.

With the rapid expansion of digital services and the increasing reliance on information systems, the continuity, security, and protection of PAHW's data assets have become critical priorities. As part of its digital transformation strategy, PAHW aims to implement a robust and modern Enterprise backup and disaster recovery solution to safeguard its mission-critical data and services.

2. Scope of the work

The Public Authority for Housing Welfare (PAHW) is seeking proposals for a comprehensive Enterprise backup and disaster recovery solution that includes:

1. Deployment across a Main Site and a Disaster Recovery (DR) Site.
2. Backup services for 1800 Microsoft 365 users, ensuring full protection of Exchange Online, OneDrive, SharePoint online, and Microsoft Teams data.
3. Ensure the protection and recoverability of PAHW's data.
4. Strengthen the Authority's resilience against cybersecurity threats, natural disasters, and operational disruptions.
5. Align with best practices in data protection.

The solution must provide:

1. Data deduplication for storage optimization.
2. Enterprise Backup and recovery services monitoring and SLA measurement.
3. Isolated Recovery to ensure recovery in case of ransomware or cyberattacks.
4. Operate fully on-premises.
5. Immutable Backup Storage to prevent unauthorized changes to backup data.
6. Enterprise Backup services for 1,800 Microsoft 365 users, covering Exchange Online, OneDrive, SharePoint online, and Microsoft Teams data.
7. All 42U cabinets (racks) with PDU required to implement the solution at both the main site and the DR site.
8. Implementation, full operation, Support, and Maintenance.
9. Training and Knowledge Transfer

3. PAHW Environment Overview

The Public Authority for Housing Welfare (PAHW) operates a robust IT environment that supports mission-critical applications, enterprise databases, file systems, and Microsoft 365 cloud collaboration platform. The proposed backup and disaster recovery solution must integrate seamlessly with this existing infrastructure, ensuring reliable protection of all current workloads while also providing the scalability and flexibility required to accommodate future growth and evolving business needs.

1. **Primary Data Center**: Located at PAHW Headquarters in south Surah (Ministries zone), hosting core applications, databases, and virtual infrastructure.
2. **Disaster Recovery Site**: Remote DR location designated to host replicated workloads for business continuity.
3. **Virtualization Platform**: VMware and Hyper-V used for majority of virtual servers and services.
4. **Storage Systems**: Dell EMC and Oracle ZFS.
5. **Databases**: Oracle **(**version 12C and above) and Microsoft SQL Server **(**2012 and above).
6. **Operating Systems**:
   - Related to the servers the solution must support Windows Server starting from 2003 (both 32-bit and 64-bit), all version Linux (both server and client), All versions of HPUX and All versions of Sun Solaris.
   - Related to desktop OS all Windows versions starting from Windows XP (both 32-bit and 64-bit).
7. **Microsoft 365 E5 Integration**:
   - 1,800 licensed users
   - Exchange Online, OneDrive, SharePoint online, and Microsoft Teams data.

4. Technical Requirements

The hardware and software components must be provided by **the same vendor (the same brand**) to ensure full compatibility, optimized support, and unified management.

4.1 Backup Storage Appliances

1. Minimum usable capacity storage per appliance must be at least 130 TB.
2. Support for data deduplication and replication across sites.
3. High availability and seamless replication features.
4. High Scalability to support growth at least for 6 years.
5. For the future expansion the appliance must support capacity expansion through additional storage shelves without requiring a complete replacement of the main system.
6. Replication between sites with automatic or on-demand failover.
7. The solution must achieve the shortest possible Recovery Time Objective (RTO).
8. The solution must achieve the lowest possible Recovery Point Objective (RPO).
9. Bidders must specify achievable RTO and RPO in their proposals.
10. Support 10 Gbps to 100 Gbps network connectivity.

4.2 Backup Software

1. Licensing for minimum 45 TB Front-End Capacity (expandable), covering on-premises servers, applications, databases, and file systems and must accommodate an estimated annual data growth rate of 10%.
2. Integrated deduplication and immutable backup.
3. Backup solution must initially operate On-Premises.
4. Backup software should support all PAHW environment (as mentioned).
5. Support for backup and recovery of Active Directory and MS exchange is must (including Granular recovery).
6. The backup software must allow central monitoring and reporting of backup/recovery operations.
7. All recovery operations for files and file systems must be easy, straightforward and single-step.
8. When capacity limits overflow observed on the backup appliance, the backup software should allow an easy-to-use method for tape-out.
9. Pre-set schedules for Tape Out must be configurable.
10. The backup software should allow individual administrative profiles for different backup and recovery administration roles.

4.3 Microsoft 365 Backup Services

1. Full back up services for 1800 Microsoft 365 users with at least 40 GB capacity per user.
2. Coverage includes Exchange Online, OneDrive, SharePoint online, and Microsoft Teams data.
3. Microsoft 365 backup is considered separately and in addition to the 45 TB Front-End Capacity licenses mentioned for on-premises workloads.
4. Microsoft 365 backup Must support granular recovery.

4.4 Cyber Recovery and Isolation

The proposed solution must include support for a dedicated Cyber Recovery Vault, serving as an isolated and secure repository for critical backup copies. This vault must:

1. Be physically isolated from the production environment.
2. Support the creation of immutable backup copies that cannot be deleted or modified for a defined retention period.
3. Be designed to protect against ransomware attacks and cyber threats.
4. Provide automated workflows for data vaulting, integrity verification, and recovery testing.
5. the vault must be completely segregated from other networks, managed independently, and physically separated in terms of power and network connectivity to ensure protection from any threat affecting the production environment.

4.5 Backup Retention Policy Requirements

1. The solution must support flexible configuration of backup retention periods at multiple levels such as daily, weekly, monthly, and yearly and allowing adjustment based on PAHW policies and business requirements.
2. The system must allow the definition of different retention policies depending on data type or workload (e.g., databases, file systems, Microsoft 365).
3. The retention policy must ensure the ability to meet regulatory and audit requirements by providing a secure and reliable mechanism for storing data for future reference when needed.
4. The solution should support the creation of immutable backup copies that cannot be altered or deleted during the retention period, enhancing protection against accidental deletion or tampering.
5. Backups should be configurable to support different data retention levels.

4.6 Reliability and System Availability

1. All components of the backup system must be hot-swappable and not require downtime if service on one of them is required.
2. Disk Shelves should have dual connectivity to the controller.
3. The backup system must have battery backed-up NVRAM.

4.7 Backup Data Integrity Management

1. Backup solution must have an architecture which ensures Data Invulnerability. Please provide proof of data invulnerability system via a whitepaper.
2. Backup solution must have the capability to continually verifying that the data stored on the system can be accessed, re-assembled and presented in its original form. The system must have capability to notify the customer in the event this verification process discovered a discrepancy.
3. All data blocks must be checked for consistency.
4. Backup solution is expected to provide this capability without any impact on performance or functionality.
5. The deduplication system must actively verify RAID stripe integrity as part of its integrity management.
6. System must be capable of providing reporting in the event of a failure.

4.8 Database Backup Support

1. Comprehensive Support for Enterprise Databases:

   - Seamless integration with Oracle Database using RMAN for efficient, catalog-aware backups.
   - Support for Microsoft SQL Server, including granular recovery at the database and item level.

2. Advanced Data Protection Features:
   - Ensures application-consistent backups, along with data compression and point-in-time recovery for critical databases.
3. Agent-Based Oracle Integration:
   - A dedicated backup agent is installed on the Oracle database server, enabling direct communication with RMAN and enhancing backup and restore operations.

4.9 Failure Handling and System Resilience

1. Automatic failure detection, alerting, retries, and escalation.
2. Clear failure recovery plan must be provided.
3. Data consistency and integrity must be ensured post-failure.

4.10 Management and Reporting

Centralized monitoring and reporting system that delivers the following capabilities:

1. Monitoring of backups and restores.
2. GUI monitoring console (web based).
3. Real-time alerts and notifications.
4. Backup & Recovery Compliance reports.
5. End-to-End backup and recovery troubleshooting analysis.
6. In-built Analysis Engine for correlation of backup statistics collected.
7. Reporting on Oracle database sizes and usage patterns.
8. Exposure reports (i.e. related to risks).
9. Clear reporting for completions or errors of Systems backup.
10. Capacity analysis and management reports.
11. Device utilization reports and statistics.
12. Monitoring and reporting system must support leading deduplication technologies.
13. Solution must provide detailed reporting on data deduplication statistics.
14. System must be capable of generating daily system performance and health reports.

4.11 Backup and Recovery Connectivity Requirements

1. Default operations must occur over secure private network connections.
2. Backup and recovery traffic must not use public Internet.
3. Direct unsecured Internet-based operations are prohibited.

4.12 Hardware and Software Freshness

1. All devices must be recent models and have been released to the market within the last three (3) years. (proof)
2. Solution Must be supported by the manufacturer for at least (6) years from the project start date. EOSL not before 6 years. (proof)
3. The bidder must propose the latest versions of required software and hardware at the time of bidding.

4.13 Ownership and Registration Requirements

1. All hardware appliances, software licenses, and related components must be brand new and should officially registered and licensed directly by the original manufacturer (OEM) in the name of PAHW.
2. bidder must provide:
   - OEM-issued ownership confirmation.
   - Software license certificates listing PAHW as licensee.
   - Warranty registration documents naming PAHW.
3. All hardware spare part replaced should be original and brand new from respective hardware vendor.
4. Third-party registration is not accepted.

5. Support and Maintenance Requirements

1. Support must be from back to back vendor.
2. Bidder must have qualified staffs that are capable of Support and Maintenance of proposed solution.
3. Bidder must have 24x7 support managed by a professional technical team.
4. Bidder should submit Help Desk/Call Center Details including level of escalation and staff details.
5. Scheduled System Health Checks and Updates:
   - During the **first year**, comprehensive on-site visits will be conducted **monthly** to perform system health checks and apply all required updates. For the **subsequent two years**, these visits will continue on a **quarterly basis**, ensuring ongoing system stability, performance optimization, and the implementation of all necessary updates and patches throughout the full term.
   - Submission of detailed technical health check reports.

6. Proposal Submission Requirements

1. Detailed technical specifications and architecture diagrams.
2. The hardware and/or software requirements for the proposed solutions.
3. Complete Bill of Materials (hardware, software, services).
4. Project plan and implementation schedule.
5. Detailed training plan.
6. Implementation and testing details.
7. Warranty throughout the period of the contract of all the required hardware and software solution.
8. Support letter confirming that bidder will offer vendor support and warranty for proposed solution.
9. Complete details on the support services (such as Help Desk and Call Center details) including staff details, Support Coverage, Escalation Procedures and SLA.
10. All required proofs that mention in the RFP.

7. General requirement

The bidding company should meet the following requirements and qualifications. Failure to do so will disqualify the bidder and his bid will be rejected.

1. Bidder must be registered with Central Agency of Information Technology (CAIT) with a valid proof upon submission.
2. The bidder must be a certified partner of the proposed backup and disaster recovery solution and hold a minimum partnership level of Gold (or equivalent). Proof of partnership status must be provided as part of the bid submission.
3. Bidders must demonstrate at least two (2) successful government backup projects using the same proposed technologies.
4. Bidder is responsible for delivering the necessary hardware and software for the project.
5. Bidder is responsible for providing all necessary cables and wiring required for the full implementation of the project to ensure immediate operational readiness.
6. Bidder is responsible for performing the installation, implementation, configuration, and testing under the vendor supervision.
7. At least 2 specialized and experienced engineers of all the proposed solutions and conducted tests for implementing the project. All proposed staff shall be under bidder sponsorship during tender submission (civil ID for each engineer has to be attached in the proposal).
8. The bidder must have a dedicated project management team to do the installation, implementation, integration and testing and a different service to maintain the solutions during the contract period. Organization chart must be submitted as evidence.
9. Bidder must submit list of the involved project and support teams showing each member skills, certificates, and description for his contribution in the project. CVs, civil IDs, and certificates of all the staff must be submitted with the tender submission.
10. Bidder must have qualified staffs that are capable of support and maintenance of the proposed solutions.

11. The bidder should agree on a scheduled site visit to check the appliances and perform any upgrades.
12. The project must be accomplished and maintained by the bidder. Third parties are prohibited during all the project phases.
13. Handing over the project will be subject to inspection; testing and acceptance of all items by PAHW technical staff.
14. Training and knowledge transfer to PAHW engineers will also be the responsibility of the bidding company during the support period.

8. Training and documentation

1. The bidder shall provide comprehensive training for at least (4) employees nominated by the Information Systems Department at PAHW.
2. Training must be conducted on-site at PAHW's premises, ensuring a tailored and interactive learning experience.
3. The training shall include hands-on practical sessions covering all components of the solution, including:

   - System operation
   - Backup configuration and execution
   - Monitoring and alert management
   - Reporting and analytics
   - Troubleshooting procedures
   - Full recovery processes

4. The bidder is responsible for ensuring that trainees gain the necessary skills to independently operate, manage, and maintain the complete backup and disaster recovery solution.
5. The bidder must submit a detailed training plan as part of the proposal, outlining schedule, curriculum, and delivery method.
6. The following documentations to be submitted to PAHW by the bidder:

   - Installation Document (Customized to PAHW)
   - Step by step instructions and manual for installing and implementing the proposed solutions (screenshots are preferable with description).
   - Official vendor administration document.
   - Solution handover and Project Closure.
   - On-demand Q&A sessions before, during, and/or after the implementation.