شركة الحوسبة الصحية

Electronic Health Solutions

REQUEST FOR PROPOSAL

Backup and Data Protection Solution

For Hakeem Program

RMS and MOH

RFP Reference Number: RFP-EHS-PROC-02-2024

Table of Contents

Transmittal Letter

Date: 22-FEB-2024

Dear Sir / Madam,

Electronic Health Solutions “EHS” is in the process of tendering “**RFP-EHS-PROC-02-2024**” for Supply, Installation, Configuration, Testing and Implementation of the **RMS & MOH- Backup and Data Protection Solution For Hakeem Program.**

Interested companies are encouraged to submit their technical and financial proposals as per the details provided in this RFP. EHS appreciates your timely and accurate response, meanwhile, shall you have any questions please do not hesitate to contact us.

Procurement Department

Tel: +962 6 580 0461 | Ext. 3050, 3071, 3074 & 3067

Email: procurement@ehs.com.jo

Yours sincerely,

Electronic Health Solution

Confidentiality Statement

This Request for Proposal (RFP) contains information proprietary to Electronic Health Solutions, hereafter referred to as “EHS”. Each recipient is entrusted to maintain its confidentiality. The information contained in this RFP is provided for the sole purpose of permitting the Bidder to respond to the RFP. This information may not be reproduced in whole or in part without the expressed written permission of EHS.

The recipient shall hereby agree to keep all the information in this RFP confidential and shall not, without prior written permission of EHS, disclose this information to any person other than the employees, agents, subcontractors, and advisors who are required in the course of their duties to execute proposal preparation activities. The recipient shall undertake the responsibility that all such persons are informed of the confidential nature of the information.

No recipient of this RFP shall, without the prior consent of EHS, make any public statements to any third parties in relation to this RFP or the subsequent short-listing of any prospective implementer or the subsequent awarding of any order. Unauthorized release of information or public statements will result in immediate disqualification.

Information provided by each Bidder will be held in confidence and will be used for the sole purpose of evaluating a potential business relationship with the respective Bidder’s company.
There will be no obligation to maintain the confidentiality of any information that was known to EHS, prior to the receipt of a proposal from the Bidder, or due to becoming publicly known through no fault of EHS, or if received without obligation of confidentiality from a third party owing no obligation of confidentiality to the Bidders.

Company Abstract

Company Profile

Electronic Health Solutions (EHS) was founded in 2009 as a non-profit company. EHS is owned by the main stakeholders in health and technology sectors in the Kingdom including Ministry of Health (MoH), Ministry of Information and Communication Technology (MoICT), Royal Medical Services (RMS), King Hussein Cancer Center, King Hussein Institute for Cancer and Biotechnology, Royal Health Awareness Society and Private Hospitals Association.

Hakeem is Jordan's National Electronic Health Records (EHR) initiative by which the healthcare sector will be computerized. The program was incepted in October 2009.

The company's mandate is to implement Hakeem in public hospitals, Royal Medical Services sites, Universities Hospitals and King Hussein Cancer Center, in addition to healthcare centers including comprehensive clinics and primary clinics.

Vision, Mission, Goals, and Objectives

Vision

Transform and sustain a continuously improving healthcare system in Jordan by leveraging information technology.

Mission

Provide a secure and accessible platform that enables the storing and sharing of electronic patient health records at all healthcare facilities enrolled in Hakeem.

Objectives

EHS main objectives are the following:

1- Improve Healthcare
2- Reduce the Cost of healthcare services.
3- Provide Data for Research and Decision Making

Benefits

- Raising healthcare quality and outcomes by enhancing the accuracy of diagnoses, medication administration, and patient information management;
- Boosting health facilities' efficiency and workflow by saving time and reducing errors in information retrieval;
- Supporting research, scientific studies and, decision-making by supplying the necessary patient data, history and statistics;
- Reducing operating costs by optimizing resource utilization and, preventing lab test repetition.

1. Contact Information

Any questions regarding this RFP shall be directed to the following email address in writing:

Name:	Procurement Department
Company:	Electronic Health Solutions
Address:	King Hussein Business Park, King Abdullah the second street. 4408 Amman 11952
Telephone / Fax:	Telephone +962 (6) 5800461 EXT3050, 3071Fax +962 (6) 5800466
Email:	Procurement@ehs.com.jo

The bidder should receive a response from the procurement department, if not please call the following number +962 79 668 1595 Or Tel: +962 6 5800461 | Ext: 3050, 3071.

2. General Conditions

Upon participation, the bidder agrees to the following:

1. All costs incurred by Bidder in the preparation of this proposal shall be borne by the Bidder.

2. "EHS" will assume that all statements in writing, made by persons submitting Proposals are true, accurate, complete and, not misleading.

3. "EHS" reserves the right to cancel, at any time, this RFP partially or in its entirety. No legal liability on the part of "EHS" for payment of any kind shall arise and in no event will a cause of action lies with any bidder for the recovery of any cost incurred in connection with preparing or submitting a proposal, in response hereto all efforts initiated or undertaken by the bidder shall be done considering and accepting this fact.

4. Bidder's proposals shall be based on full compliance with the terms, conditions and, requirements of this RFP and its future clarifications and/or amendments.

5. "EHS" shall not be under any obligation to return or save either the original or any copies of any Bidder's Proposals (technical and/or financial), and all documents submitted to "EHS", whether originals or copies, shall be kept or disposed of by "EHS".

6. This Request for Proposal doesn't constitute an offer. "EHS" shall not be under obligation to enter into any agreement with any Bidder in connection with this RFP and responses received.

7. The Bidder's proposals (technical and financial) shall comply with the laws and regulations of the Hashemite Kingdome of Jordan.

8. The Bidder's proposals (technical and financial) shall be compatible with international standards and best practices.

9. As a part of the RFP response, the Bidder is requested to fill out the compliance sheet included in this RFP.

10. The bidder must include in his technical proposal a detailed Bill of Quantity "BOQ" for all proposed and priced items and services. Accordingly, this should be reflected and included in the financial offer with itemized quoted prices for all proposed items.
11. The bidder must commit to providing EHS with the same prices and terms for a period of (1) year starting from the Awarding Letter date for the purpose of Variation Orders

12. The quantities requested in this RFP are subject to increase, decrease or, cancellation as per the actual requirements in the awarding date. In case the quantities decrease the vendor is responsible to install the available materials from the EHS warehouse.

13. في حال أن تعذر على "المناقص الفائز بالعطاء" تنفيذ التزاماته التعاقدية و/أو أي جزء منها، بحيث يكون قد تأخر في توريد المواد و/أو الخدمات المحددة لمدة (45) يوم من التاريخ الواجب على " المناقص الفائز بالعطاء " خلاله تنفيذ التزاماته، فسيكون في هذه الحالة من حق "شركة الحوسبة الصحية" إلغاء قرار الإحالة والعلاقة التعاقدية التي تجمعهم مباشرة دون الحاجة الى اشعار و/أو انذار و/أو استصدار حكم قضائي. كما يكون من حق " شركة الحوسبة الصحية " في هذه الحالة شراء ما كان متفق عليه من مورد آخر يراه مناسبا، على أن يتحمل " المناقص الفائز بالعطاء " كافة النفقات التي قد تكبتدها " شركة الحوسبة الصحية " جرّاء ذلك الى جانب تعويض " شركة الحوسبة الصحية " عما لحقه من أضرار إثر تعذر "المناقص الفائز بالعطاء" عن تنفيذ إلتزاماته.

3. Bidder Qualifications

1. Bidder should be a Company registered under the Jordanian Ministry of Industry and Trade for more than three years or represented by a company abiding by the aforementioned condition; otherwise, any international or regional bidder must present the formal documents which prove the financial capacity of the company in addition to its commercial registration documents at the country of origin
2. Bidder should have at least three references of similar projects preferably in the health care sector and to be accepted by EHS.
3. The Bidder shall have at least 2 live installations with support as of the date of submission of this bid.
4. The Bidder shall have specialized and certified engineers with relevant technical certification for at least two engineers.
5. The bidder must submit Up-To-Date official documents of registration issued from the Companies Control Department at the Jordanian Ministry of Industry and Trade.
6. The bidder shall be an authorized Top Level Partner of the mother company he represents in this bid. An up-to-date valid official letter/certificate from the mother company shall be submitted by the bidder as part of the bidder's qualification documents, to prove the level of partnership for the bidder.
7. The bidder must have at least (2) two engineers certified by the mother company for the implementation and technical support of the proposed solution.
8. All proposed and supplied equipment\solutions\items\services must be original, brand new (not refurbished) and, licensed by the manufacture (mother company) to be supplied and installed for this project at EHS.
9. All proposed and supplied equipment / solution / items / appliances / hardware must be newly manufactured with manufacturer valid warranty and support duration for not less than (7) years from the date of delivery. This implies that supplied products must not be obsolete, phased out of production, out of sales, and support.
10. All proposed and supplied equipment\solutions\items\services must be original, brand new (not refurbished) and, licensed by the manufacture (mother company) to be supplied and installed for this project at EHS.
11. تلتزم الشركة المحال عليها بتحديد نسبة الصيانة و الدعم الفني في العرض المالي للأجهزة المحال عليها للسنوات التي تلي فترة الصيانة المجانيةشاملة قطع الغيار و الأيدي العاملة علماً بأن هذا البند سيكون جزء من التقييم المالي للعرض المقدم

The winning bidder is obliged to determine the percentage of maintenance and technical support including spare parts and manpower for the years following the free maintenance duration. This has to be specified clearly in the financial offer for the supplied devices\solutions as per this RFP and will be part of the financial evaluation of the bid.

12. The bidder shall classify as a tier one partner; the bidder shall provide the required manufacturer’s certificates or letters for his qualifications.
13. The bidder must provide end of sale / end of life information about the proposed solution(s) as provided by the manufacturer. Such information shall be submitted as part of the official submittals and will be part of the evaluation criteria.
14. All HW components should be new, Original from the Vendor (all components should have original part number from the vendor), and vendor factory integrated.
15. The bidder shall provide the yearly cost of the vendor's support service for additional two years.
16. The bidder shall provide a local stock for spare parts to meet the SLA requirements.
17. The bidder must include their Project Management Methodology and their Project Management team’s CVs.
18. The bidder must submit up-to-date official documents of registration issued from the Companies Control Department.

4. RFP Guidelines

a. RFP Issuance & Submission

Event	**Date**
1. RFP distribution to vendors	22-FEB-2024
2. Questionnaire Session	N/A
3. Proposal due date Closure Date	14-MAR-2024

b. Queries and Responses

All inquiries during the questions and answers session (Bidder Conference) if conducted must be documented., Verbal clarifications, inquiries or communication are not permitted, and only written communication is accepted.

c. RFP Acknowledgement

1. Award of the contract resulting from this RFP will be based upon the most responsive vendor whose offer will be the most advantageous to "EHS" in terms of cost, functionality, and other factors as specified elsewhere in this RFP.

2. Vendor has a period of (5) days to acknowledge and accept the awarding letter with its terms and conditions. Delay of acceptance will yield into consideration of rejection.

3. EHS" reserves the right to:

   a) Accept other than the lowest-priced offer.
   b) Award a contract on the basis of initial offers received, without discussions or requests for best and final offers.
   c) Award the RFP contract on a partial basis (i.e. not all requirements requested from a single vendor.)
   d) Not declare the name of the winning bidder, and awarding details.

d. Proposal Format Requirements

1. The financial and technical proposals must be submitted separately. Each proposal must be sent in a separate (PDF) electronic file (PDF). (**If the proposal file document size is bigger than 9 Megabyte (MB), you may send the document through a secured file hosting service and an internet-based computer file transfer service company such as Dropbox, WeTransfer, etc.**)
2. The proposals must be sent to the Procurement Department email namely; (Procurement@ehs.com.jo). A password divided into (3) portions and not to be less than (9) nine digits must be set on the financial offer.

3. The passwords must be sent through a text message (SMS) to relevant mobile numbers which will be cellular mobile numbers that will be provided to the bidders at a later stage.
4. Pricing must be per site with a breakdown itemized pricing for each item, component, product and services included in the submitted Financial Proposal.
5. The Financial Proposal must specify clearly the compliance with the (5) five years' warranty duration required in the Technical Specification section.

6. The bidder shall submit only one financial proposal file. The financial proposal must include all of the products or solution options proposed in the Technical Proposal. The financial proposal must be in a format that is easy to read and understand and in compliance and consistent with the pricing and terms and conditions mentioned in this RFP document. The financial proposal must be in English.

   The financial proposal must be signed by an authorized representative of the bidder.

   If the bidder submits more than one financial proposal file, or if the financial proposal does not include all of the products or solution options proposed in the Technical Proposal, the bidder's proposal may not be considered.

7. The bidder must submit a cover letter in a PDF format as a separate document from the Technical and the Financial Proposal. The cover letter must include the following information:

   - The tender reference number.
   - The name of the bidder.
   - The contact information for the bidder.
   - A list of the product(s) and\or solution(s) names that are being proposed, along with the corresponding product and/or solution code.
   - A listing of the proposed product(s)\ solution(s)\service(s) along with their relevant brief description.

The aforementioned information must be filled in the following "Table Template" and must be consistent and in a total match with the relative names and descriptions included in the financial and technical proposals.

The list of product and/or solution names must match those included in the Technical and Financial Proposal. If the bidder does not submit a cover letter, or if the list of product and/or solution names do not match those included in the Technical and Financial Proposal, the bidder's proposal may not be considered.

Table Template (ملخص للمنتجات والخدمات والحلول المعروضة)

The following table template can be used to list the product and\or solution names that are being proposed:

Option	Product\Solution\Services Name	Product\Solution\Services Description
Option (1)	**Product 1**	
Option (2)	**Solution 1**	
Option (3)	**Solution 2 & Product 2**	

5. RFP Terms & Conditions

a. Evaluation Criteria

1. "EHS" will evaluate each response. Responses will be evaluated on many criteria deemed to be in EHS's best interest, including but not limited to, technical offering, price, warranty, delivery duration, Bidder certification, accreditation, schedule, bidder's capabilities, compliance with bonding, and any other factors that "EHS" determine. The order of these factors does not denote relative importance.
2. "EHS" reserves the right to consider other relevant factors as it deems appropriate in order to obtain the best value.
3. This RFP does not commit "EHS" to select any firm, enter into any agreement, pay any costs incurred in preparing a response or procure or contract for any services or supplies. "EHS" reserves the right to request additional information from the bidders whose response meets "EHS" needs and business objectives without requesting such information from all respondents.

b. Rejection of Proposals

"EHS" reserves the right to reject any or all offers and discontinue this RFP process without obligation or liability to any potential Vendor.

c. Proposal Costs and Expenses

No legal liability on the part of "EHS" for payment of any kind shall arise and in no event will a cause of action lies with any bidder for the recovery of any cost incurred in connection with preparing or submitting a proposal. In response hereto all efforts initiated or undertaken by the bidder shall be done considering and accepting this fact.

d. Bid, Performance, Advance payment, and Warranty Bonds

1. Unconditional Bid Bond valid for (3) three months with an amount of (JoD 9,000.00) Nine Thousand Jordanian Dinar to be renewed automatically must be submitted by every participating bidder.

2. Advance payment LG, is to be submitted against any required advanced payment.

3. Unconditional Performance Bond for (10%) of the total amount of the awarded value shall be submitted by the winning bidder and within (5) working days from the date of the award. The Performance bond must remain valid for the total duration of the implementation of the project and until the delivered solution is finally received and accepted by EHS. This Performance Bond will be replaced by the Maintenance LG after items delivered installed and finally accepted duly. The Maintenance Bond will remain valid until the end of the warranty duration. In case the winning bidder fails to submit the performance bond, EHS reserves the right to cancel the contract and liquidate the bid bond without reverting to the bidder.

e. Penalties

In the event, the bidder fails to deliver according to the agreed time (for either the initial agreed delivery date or any of the subsequent delivery dates). The Bidder must pay EHS a delay penalty of (1%) of the total contract amount for each calendar week of delay. The maximum penalty for delays shall not exceed (10%) of the total contract value. The payment or deduction of such penalty shall not relieve the winning bidder from its obligations to complete the services or from any other obligations and liabilities under this bid.

f. Payment Terms

1- Payment terms:

20% Advance Payment against "Advance Payment LG"
20% upon items delivery
20% upon installation or implementation
40% on final EHS acceptance.

In case the winning bidder fails to comply with the "Advance Payment LG" term set for the first payment, hence, the winning bidders will be entitled to receive (40%) of the total contract value after the fulfillment of the delivery and initial receiving conditions "إستلام توريدي" set forth in this RFP.

2- Payment currency shall be in Jordanian Dinar (USD and Euro exchange rate will be calculated at the currencies exchange rate issued by Central Bank of Jordan at the payment date).

g. Terms of Delivery

- Delivery, Installation and, Implementation within (8-12) Weeks from the date of the purchase order at the EHS HQ offices or any of "Hakeem" Project sites. Final acceptance is required by EHS, and penalties for delays will be imposed as per the condition specified in clause (5.e) of this RFP.

h. Offer Expiry Date

The validity of the Proposal shall be no less than (90) days unless clearly mentioned differently.
The prices must remain fixed and valid for (90) days from the date of the invitation for bid closing date and shall be clearly stated in the technical and commercial bids.

6. Financial Compliance Sheet

#	Description	Comply (Yes/No)	Reference in the proposal
1	The bidder shall comply with all points included in the general conditions section		
2	The bidder shall comply with all points included in the bidder qualifications section		
3	The bidder shall comply with all points included in the RFP guideline section		
4	The bidder shall comply with all points included in the RFP terms and conditions section		

7. Objectives

EHS invites technically complete and commercially competitive bids from reputed bidders for the Supply, Installation, Configuration, Testing, and Implementation of Data Protection Solution for Hakeem datacenters in Royal Medical Services (RMS) and Ministry of Health (MOH).

The winning bidder will be solely responsible for the complete **Supply, Installation, Configuration, Testing, and Implementation of a Backup and Data Protection Solution for the Hakeem Program across two separate lots**:

- Lot (1): Royal Medical Services (RMS) datacenter
- Lot (2): Ministry of Health (MOH) datacenter

8. Lot (1): Business Requirements- RMS

From a business perspective, the new Data Protection Solution must be delivered as a robust, enterprise-grade turnkey solution meticulously tailored to align with EHS requirements and uphold industry standards for backup, data protection, disaster recovery orchestration, and cybersecurity recovery systems. This imperative encompasses a comprehensive approach addressing the following key points:

1. **Backup and Data Protection:**
    1. Data Source Compatibility: Ensure compatibility with diverse data sources, covering databases, virtual machines, containerized applications, applications, and file systems.
    2. Global Deduplication: Implement global deduplication to optimize storage utilization and reduce redundancy across data centers.
    3. Encryption: Provide end-to-end encryption for data in transit and at rest to meet security and compliance standards.
    4. Scalability: Scale seamlessly to accommodate the enterprise's growing data volumes and diverse workloads.

2. **Disaster Recovery Orchestration:**
    1. Automated Failover and Failback: Enable automated failover and failback procedures for quick and efficient disaster recovery.
    2. RTO and RPO Compliance: Ensure adherence to Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements According to ISO 22301.

3. Cross-Data Center Synchronization: Facilitate real-time or near-real-time synchronization between main and DR data centers.
4. Testing and Validation: Allow for non-disruptive testing of disaster recovery plans that is related to ISO 22301 to validate their effectiveness.

3. Cybersecurity Recovery:

1. Air-Gapped Backups: Support air-gapped backups to create a physically isolated copy of critical data to protect against cyber threats.
2. Immutable Backups: Implement immutability features to prevent unauthorized modifications to backup data.
3. Incident Response Integration: Integrate with incident response systems (such as IBM security SOAR (Security Orchestration, Automation and Response, and others) to enhance the organization's ability to counter cybersecurity threats.
4. Ransomware Detection and Mitigation: Provide advanced capabilities for ransomware detection, mitigation, and recovery.

4. Compliance and Reporting:

1. Audit Trails: Maintain comprehensive audit trails for backup, recovery, and disaster recovery operations.
2. Regulatory Compliance: Ensure compliance with regulations and data protection laws.
3. Customizable Reporting: Generate customizable reports on backup success, recovery points, and disaster recovery testing results.

5. Management and Monitoring:

1. Centralized Management Console: Offer a centralized console for configuring, monitoring, and managing backup and recovery operations.
2. Alerting and Notifications: Provide real-time alerts and notifications for any anomalies, failures, or breaches.
3. Role-Based Access Control: Implement role-based access controls to restrict access to sensitive backup and recovery functionalities.

6. Integration and Compatibility:

1. API Integration: Support APIs for seamless integration with other enterprise systems and workflows.
2. Third-Party Integrations: Integrate with third-party tools and solutions for broader security and operational capabilities

7. **Support and SLAs:**
    1. 24/7 Technical Support: Ensure round-the-clock technical support for critical issues and emergencies.
    2. Service Level Agreements (SLAs): meet SLAs for backup, recovery, and disaster recovery timeframes according to the best practice and ISO 22301

8. **Cost and Licensing:**
    1. Transparent Pricing: Provide transparent pricing models with clear licensing terms and scalability options.
    2. Total Cost of Ownership (TCO): Consider the TCO, including hardware, software, and operational costs, for an accurate financial assessment.

9. Lot (1): Submittals - RMS

The bidders' proposal shall include the following:

1. Compliance sheets (for both technical and financial).
2. Data sheets for all items.
3. Project Implementation plan.
4. Accept Procedure Test (ATP) document.
5. Service level agreement (SLA)
6. Project team details.
7. Detailed BOQ (Item, QTY, and Duration)

10. Lot (1): RFP Objective - RMS

The objective of this RFP is to solicit proposals for the installation of an enterprise-level data protection solution in both the main and disaster recovery (DR) data centers. The selected solution should align seamlessly with our comprehensive business requirements, ensuring robust protection for databases, virtual machines, containerized applications, applications, and file systems.

The overarching objective is to identify a vendor capable of delivering a turnkey solution, expertly installed in both the main and DR data centers, ensuring the highest level of data protection, recovery, and resilience for EHS.

11. Lot (1): Solution Technical Specifications - RMS

11.1. Solution High-level Architecture

The proposed solution is envisaged to be seamlessly deployed across both King Husain Medical City (KHMC) (Main) and King Talal Military Hospital (KTMH) (DR) data centers, strategically addressing the imperative for High Availability (HA), Disaster Recovery (DR), and protect and recover against ransomware with threat protection capabilities. The prospective bidder is expected to intricately design and present a comprehensive solution architecture tailored to meet the unique demands of our main and DR data centers, while diligently accommodating the critical High Availability requirements.

This architecture should not only ensure the robust functioning of the system under normal operational conditions but also guarantee a swift and effective transition to the Disaster Recovery environment in the event of any unforeseen disruptions. Furthermore, the bidder's proposal should include a robust Cyber Recovery framework, incorporating best practices to safeguard critical data against cybersecurity threats. The proposed solution should outline a resilient framework that aligns seamlessly with the High Availability, Disaster Recovery and Cybersecurity Recovery mandates, ensuring the utmost protection and recoverability of our essential data assets.

During the project lifetime (minimum of five years), all the provided solution components and services (control and data planes) must reside within Hakeem program datacenters without the need to host / use any cloud based services or components, excluding the software and the definition updates.

For an effective data protection solution, it is best to get backup software, a backup appliance, and cybersecurity recovery from one vendor. This makes support simpler and ensures everything works smoothly together. A unified system reduces the chance of compatibility problems and is easier to manage. With one point of contact for support, issues get resolved faster, avoiding the complications of dealing with multiple vendors. This approach not only improves the reliability and performance of the data protection system but also makes it easier for users to manage and troubleshoot.

11.2. Backup and Data Protection Solution Technical Specifications

The Solution must offer effective capabilities to simplify management of data protection across complex enterprise environments. It must also ensure reliable recovery by protecting backup data against a constantly changing threat landscape, and expedite and orchestrate data recovery responses to traditional disaster and ransomware events. Below are the minimum technical specification for the solution:

11.2.1. Backup and Recovery Software

1. Comprehensive Backup and Recovery solution that provides flexible deployment options to ensure fast, secure backup and recovery for cloud, remote offices, and data center with client-side data deduplication.
2. Solution should create application-consistent, image-level backups of Virtual Machines and Physical Servers, ensuring successful recovery of business-critical applications and services and allowing for application-specific restore scenarios.
3. Solution must support backup of Windows and Linux physical servers, endpoints, containerized applications and Cloud VMs.
4. Solution must support backup of entire image, volumes, or files or folders for physical servers and endpoints.
5. Solution must provide the capability to protect Virtualized platform such as VMWare, Microsoft Hyper-V, Nutanix Acropolis Hypervisor (AHV) and Red Hat Virtualization (RHV) platforms using agentless mode.
6. Solution should have the capability in divides backup data into variable-length sub-file segments, compresses and applies a unique hash identifier to each segment during the backup process.
7. Solution must deduplicate data at the client, before transfer across the network.
8. Solution must have the option to de-duplicate backup data at the target (if needed) for optimized efficiency with specific data types.
9. Deduplication technology should dramatically reduce the amount of data sent and stored - eliminating backup bottlenecks and reducing storage costs

10. Solution should determine if a segment has been previously backed up and only backs up the unique segments, greatly reducing backup times.
11. Solution must have plugins/modules to integrate with most of third-party DB technologies as necessary.
12. Solution must have a single pane of glass management software to simplify the prod and DR backup infrastructure management.
13. Solution must provide the capability to backup VMWare workloads with zero stun-effect and no downtime during the backup process.
14. Solution should provide a CDP (Continuous Data Protection) functionality to eliminate downtime and minimize data loss for Critical VMware vSphere workloads and perform immediate recoveries to a latest state or desired point in time achieving the most stringent RTO and RPO.
15. Solution should provide end-to-end encryption for Server backup and replication data in flight and at rest.
16. Must support granular restore of single email/file or other granular items directly from the de-duplicated storage on the appliance or repository without the need to duplicate or copy the backup to disk storage before restore
17. Must Support self-service recovery natively for all Applications and VMware farm
18. Solution should support VM configuration and Virtual Hard Disks restore.
19. Solution should have an intelligent load-balancing of resources that allow parallel backup of VMs to reduce backup and replication windows
20. Solution should automatically backup its configuration and it should provide a straightforward mechanism to restore the configuration in case of any failure.
21. Solution should have the ability to instantly recover VMWare VM Guest OS files from backup with no need to deploy agents in production VMs or Hypervisor before backup.
22. Solution should have the ability to view files from backups in the production Microsoft Windows file system and recover only the changed files.
23. Solution must be able to deploy software agents on systems to be protected (no extra local hardware required, just license add in the future for specific applications & databases if required).
24. Solution must reduce backup impact on client CPU.
25. Solution should be able to recover individual application items (such as databases, e-mails, sites, users) from Microsoft Exchange, Active

Directory, SQL, SharePoint, Oracle and PostgreSQL physical or virtual servers' backups.

26. Solution should have an ability to instantly start VMware Virtual Machine directly from any backup disk storage at any chosen recovery point, on same or different virtualization host.
27. Solution should have an ability to recover from an image-level backup including physical servers or workstations, virtual machines or cloud instances directly from any backup disk storage at any chosen recovery point to a VMWare vSphere, Hyper-V or AHV Virtual Machine.
28. Solution should have the ability to instantly mount disks from any VMWare Virtual Machine backup to the selected VMware VM.
29. Solution should include a Windows and Linux Guest OS file indexing feature and comprehensive OS file search engine in order to delegate file recovery operations to help desk or end users.
30. Solution should support fast VM roll-back using Changed Block Tracking (CBT) restore and restore over SAN
31. Solution should support file level, volume level, and bare-metal restore for Windows and Linux servers or workstations
32. Solution should provide instant access to the content of any backup or replica to specialized third-party mining and security analysis applications and scripts that mounts the content of any restore point into the file system of the specified application server.
33. Solution should provide automated backup verification technology for VMware vSphere, Virtual Machines and which will guarantee the recoverability of the Server at Guest OS and Application levels.
34. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.
35. Solution should perform an automated backup server configuration check against best practice guidelines to understand how backup infrastructures can be improved to address potential security concerns.
36. Solution should be able to operate in modern data centers that are configured with IPv6 networking
37. Solution should be able to track user actions and backup activities and gain complete transparency over file-level restore operations through specifically designed audit files
38. Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.

39. Solution should provide multi-tenant reporting and monitoring allowing multiple users to simultaneously access monitoring and reporting interfaces.
40. Solution must be able to monitor storage datastore utilization and capacity planning / forecasting
41. Solution should provide agentless data collection from virtualization hosts, management servers and failover clusters
42. Solution should provide alerts and reports to identify and resolve common infrastructure and software misconfigurations before operational impact.
43. Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.
44. Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events
45. Solution should support pre-defined reports and monitor location tags for VMs, hosts, computers configured in backup solution to observe data sovereignty.
46. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks
47. Solution should support multi-tenancy

11.2.2. Purpose Built Backup Appliance

1. Appliance Must be fully compatible with the proposed backup software and must support client direct backup from all servers and clients to the appliance without any need to add media agents
2. Appliance Must provide an efficient, high performance inline deduplication technology with a local compression technique
3. Deduplication process must utilize sub-file variable-length segment recognition and filtering process that works at block sizes as small as 4 kilobytes to maximize efficiency.
4. The Storage Device shall be a self-contained disk system.
5. Shall be able to support 16 or 32 Gbps FC connectivity for direct SAN connectivity if required in the future.
6. Should include a minimum of two 10/25 Gbps Ethernet ports on separate network cards with 25 Gbps transceivers, including the transceivers from network switch side (Juniper EX4650)
7. Should support Ethernet failover, Ethernet aggregation and VLAN tagging

8. Appliance Must support an internal mechanism to provide the best defense against data integrity issues to continuously verify, detect and protect against data recoverability issues throughout the life cycle of the backup data
9. Supports Distributed de-duplication processing using software Plugin on Backup Server
10. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks
11. Appliance Must Support WORM feature
12. Appliance Must support Snapshot features to make read-only copy of the backup Images for protection
13. Must provide high availability for all hardware components, such as power supplies, storage, and network interfaces. This minimizes the risk of a single point of failure.
14. Dual disk parity RAID 6 with Spare or better technique
15. Appliance should provide network-efficient, automated, ultra-safe replication for disaster recovery (DR), remote office data protection and multi-site consolidation.
16. System must be capable of supporting replication/DR requirements such that deduplicated data starts replicating when backup starts to achieve faster Recovery Point Objectives
17. Appliance Must support bi-directional, Many-to-One and cascaded replication between appliances
18. Must support management of replication at backup software level
19. Ability to access the backup images on the destination Appliance as read-only from backup servers
20. Must support bandwidth throttling for replication
21. Must have Web/Browser based Management GUI to manage multiple backup appliances from the same console
22. Must support inline data-at-rest encryption
23. Must support secure encrypted replication between appliances
24. Must support Oracle Direct RMAN backup without the need to any backup Software
25. The appliance must support Extended retentions capabilities for the long term archiving requirements
26. The appliance must support direct backup to the cloud without any need to another Hardware in the middle between the appliance and the cloud storage
27. The provided appliance shall support future increase in backup capacity to the double of the sizing space provided in this RFP
28. The provided appliance shall provide Protection against NTP Attacks

29. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.
30. Must support multi-tenancy
31. System must be capable of providing backup throughput of 25 TB/Hour

11.2.3. Cybersecurity Recovery Solution

1. Solution must provide isolated recovery backup copy that is totally physically isolated form the production network (air-gapped)
2. Hardware and Software must be compatible with the provided Hardware and Software within the Data Protection Solution
3. The solution must support creating multiple backup golden copies, by replicating a copy of backup data to a physically and logically isolated and protected vault. The golden copy must be scanned and verified.
4. The replication between the existing backup and the isolated site must be automated and must use pull technique to pull the data from the main site
5. Solution must support restore and validation workflow for the restored backup images
6. Solution must be widely deployed and tested with enterprise customers
7. Solution must support Air-gap technology
8. Solution must provide Intelligent techniques to Analyze backed up data deep analysis from Meta Data, Header & Content
9. Solution must provide machine learning and full-content indexing with powerful analytics within the safety of the vault.
10. Solution must provide automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.
11. Solution must create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production / backup environment and the vault.
12. Solution must contain workflows and tools to perform recovery after an incident using dynamic restore processes and the existing DR procedure
13. Solution must create an isolated environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance. The bidder shall provide all the required components for this isolated environment that are required to use and operate the solution according to vendor's best practice and complying with NIST SP 800-209 (Security Guidelines for Storage Infrastructure).
14. The provided solution shall provide protection against NTP Attacks
15. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password

credentials, to provide more secure access to the console and protect user accounts from being compromised.

16. Must support Retention Lock capabilities for Archive requirements and to provide the best defense against ransomware attacks
17. Solution Must support multi-tenancy

11.2.4. Disaster Recovery, Replication and Orchestration Solution

1. Solution should provide Service-level and Application-level monitoring and ensure the availability of mission-critical applications running in physical and virtual machines through enhanced, proactive application-level monitoring functionality, including the ability to track an individual application's health monitoring status as well as manage guest services and processes.
2. Solution should offer reports covering all aspects of the Virtual Infrastructure; including VM availability (uptime), trend analysis, resource utilization, infrastructure documentation and management, and change tracking - for every object in the virtual infrastructure.
3. Solution should present monitoring and reporting data from both technical and business-oriented perspectives. Business-oriented views are based on user-defined criteria and can include categorizations such as organizational structure, location, SLA, department, etc.
4. Solution should be able to overlay event data on performance graphs for viewing the effect of events on utilization and trends
5. Solution should provide visual status indicators on parent objects for at-a-glance notification of potential problems with underlying objects.
6. Solution must automate recovery planning, testing and orchestrates the steps needed to recover from a planned or unplanned disaster
7. Solution should create workflows to orchestrate recovery operations for both virtual and physical machines to VMware vSphere and public cloud environments
8. Solution should be able to automate the verification of infrastructure readiness for recovery
9. Solution must include Failover Orchestration allowing a 1-click failover for VMware VMs to avoid long downtimes.
10. Solution must enable ability to include custom scripts to be executed in the orchestrated plan
11. Solution must be able to verify the recovery plan automatically and upon schedule

12. Solution must be able to automate recovery actions from backups
13. Solution must be able to automate failover to VM replicas (Scheduled and CDP)
14. Solution must be able to automate serving data from a destination or a secondary volume
15. Solution should generate dynamic reports for orchestration plans that include a scope of orchestrated workloads, details on the recovery location, information on specific steps that will run during the recovery process, test execution details and summary information on plan test results
16. Solution should support any point-in-time recovery to avoid logical corruption and roll back to any point in time
17. Solution should support crash consistent and application consistent short term and long term replicas of virtual machines with near zero RPO
18. Solution should provide the ability to group the virtual machines and applications into logical groups and stacks
19. Solution should be able to orchestrate the recovery of virtual machines from backups and VM replicas in a defined order and with set customizable boot delays
20. Solution should provide automated Replica verification technology for VMware vSphere Virtual Machines which will guarantee the failover of Virtual Machine at VM, Guest OS and Application levels
21. Solution should provide an Intelligent VM Failover mechanism which includes Failover Plans, automated Re-IP, and network mapping of VMs on DR site and a failback technology which transfers only changed blocks back to production site.
22. Solution should provide an option to execute custom scripts before and/or after the backup or VM replication jobs.
23. Solution should provide Host based replication of EHS VMware vSphere Virtual Machines for High Availability and Disaster Recovery purposes managed from a single console.
24. Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.
25. Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events
26. Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.
27. Solution should have an intelligent load-balancing of resources that allow parallel Replication of VMs to reduce replication windows

28. Solution must have the ability to facilitate large scale recovery by creating sophisticated DR plans and automatically executing them (i.e. application-specific steps)
29. Solution should be able to create rich DR documentation, run test plans and verify application consistency
30. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised
31. Solution must support multi-tenancy

12. Lot (1): Scope of Work - RMS

The scope for delivering the Backup and Data Protection Solution shall include the following:

1. **Project Kickoff:**

    - Hold an initial meeting to align project objectives and timelines.
    - Define roles and responsibilities.
    - Develop a Project implementation plan and project schedule. The supplier shall assign a qualified technical project manager to manage the project and to ensure the controls and successful delivery.

2. **Solution Components Delivery**

    - The delivery of all the solution components to EHS Warehouse and the sites based on EHS requirements and policies, including moving the materials to and within the sites.

3. **Pre-Implementation Assessment:**

    - Perform preparatory site visits and related activities to ensure the best deployment.
    - Conduct an assessment of the existing IT infrastructure.
    - Identify specific requirements and constraints.

4. **Solution Design:**

    - Develop a detailed solution design based on the provided business requirements.
    - Include architecture diagrams, component specifications, and integration points.

- Conduct technical workshops with EHS technical team to develop the solution architecture, HLD, and LLD. The entire project's documentation must be approved by EHS.
- The solution design must be provided by the vendor end-to-end

5. **Solution Setup and Installation:**

- Deploy necessary hardware and software components.
- Configure solution's equipment.
- Follow EHS instructions in labeling all equipment and switches and put a description in the network devices configuration.
- Patching the copper and fiber patch cords cables inside the cabinets.
- Provide any extra materials or/and services required to deliver a complete turnkey solution.

6. **Integration and Compatibility:**

- Ensure seamless integration with existing enterprise systems.
- Verify compatibility with databases, virtual machines, containerized applications, and other data sources.

7. **Configuration and Optimization:**

- Configure backup software to meet EHS full requirements that are compliant with ISO27001, including but not limited to: backup policies, schedules, and retention periods.
- Optimize performance for scalability and efficiency.
- Establish disaster recovery configurations for main and DR data centers.
- Define failover and failback procedures according to EHS full requirements
- The vendor shall provide the full implementation, configuration and testing for the Cybersecurity Recovery Solution.

8. **Security Measures:**

- Implement end-to-end encryption for data in transit and at rest without any additional components from EHS
- Set up access controls and authentication mechanisms according to EHS policies

9. **Testing and Validation:**

- Conduct thorough testing of backup and recovery processes.
- Validate disaster recovery plans through simulated scenarios.

- Perform Acceptance Test Procedure (onsite) and any corrective action to collect EHS acceptance.
- The vendor must provide the final validation for the implemented solution.

10. **User Training:**

- Develop training materials for operator and IT administration staff.
- Provide training sessions to ensure proper utilization of the data protection solution.

11. **Documentation:**

- Document the implemented solution comprehensively.
- Include configuration guides, operational manuals, and troubleshooting procedures.

12. **Monitoring and Alerting:**

- Set up monitoring tools to track the health and performance of the data protection system.
- Configure alerting mechanisms for immediate issue detection.

13. **Reporting:**

- Implement customizable reporting features.
- Generate reports on backup success, recovery points, and disaster recovery testing results.

14. **Knowledge Transfer:**

- Transfer knowledge to the IT team for ongoing system management.
- Provide guidance on routine maintenance tasks.

15. **Post-Implementation Support:**

- Offer post-implementation support to address any issues or concerns.
- Conduct periodic reviews to ensure optimal system performance.

13. Lot (1): Deliverables - RMS

1. **Detailed Solution Design Document:**
    - Architecture diagrams.
    - Component specifications.
2. **Configured Solution:**
    - Deployed and configured hardware and software components.
3. **Integration Documentation:**
    - Documentation on integration with existing systems.
4. **Backup and Data Protection Policies:**
    - Configured backup policies, schedules, and retention periods.
5. **Security Documentation:**
    - Documentation on implemented cybersecurity measures.
6. **Disaster Recovery Plans:**
    - Detailed disaster recovery plans for main and DR data centers complying with EHS policies that are compliant ISO 22301.
7. **Testing Reports:**
    - Reports on testing and validation activities.
8. **User Training Materials:**
    - Training materials for end-users and IT staff.
9. **Comprehensive Documentation:**
    - Operational manuals, configuration guides, and troubleshooting procedures.
10. **Monitoring and Alerting Setup:**
    - Configured monitoring tools and alerting mechanisms.
11. **Reporting Templates:**
    - Templates for customizable reports.

12. **Knowledge Transfer Session Records:**

- Records of knowledge transfer sessions.

13. **Post-Implementation Support Agreement:**

- Formal agreement for post-implementation support. Provide the support approach in the form of signed and stamped SLA, including the escalation matrix, support contacts and response time

14. Lot (1): Bill of Quantities - RMS

The below is the BOQ for the solution included in the below table, each components sizing and license requirement is based on the below details within this section.

Item	Location	Description	Qty
1	Main Datacenter	Backup and Recovery Software	1
2	DR Datacenter	Backup and Recovery Software	1
3	Main Datacenter	Disaster Recovery and Replication Solution	1
4	DR Datacenter	Disaster Recovery and Replication Solution	1
5	Main Datacenter	Purpose Built Backup Appliance	1
6	DR Datacenter	Purpose Built Backup Appliance	1
7	Main Datacenter	Cybersecurity Recovery Solution	1

The solution sizing and capacity shall be based on the following criteria as minimum; these criteria are required for providing the needed licenses, hardware performance, and storage capacity

#	Workload	Data Growth Yearly	Daily Change	Size TB	QTY	Backup Policy
1	Virtual Machines - DB	10%	3%	5	90	1. Daily Incremental with 1 Week Retention 2. Weekly Full with 4 Weeks Retention 3. Monthly Full with 12 Months retention 4. Yearly Full with 1 Year Retention
2	Virtual Machines – File System	15%	3%	14	10	
4	Virtual Machines -	10%	3%	1	3	

	Kubernetes / Rancher					
5	Physical Server - Generic DBs	15%	3%	5	1	

- Kubernetes / Rancher platform is intended to run 20 applications
- Cybersecurity Recovery Solution to be isolated in different Purpose Built Backup Appliance with deep analysis based on technical requirements in “Cybersecurity Recovery Solution” section.
- Backup and Recovery Solution to cover all workloads mentioned above. In addition, based on the architecture described in the “Solution High-level Architecture” section.
- The bidding entity is required to furnish a comprehensive analysis of the total cost of ownership for the proposed solution delineated in this RFP. This entails presenting a detailed breakdown of the total solution cost over a ten-year span, distinctly outlined in the financial offer's separate section. The cumulative total cost of ownership should encompass the initial expenses associated with the solution, as stipulated by the RFP requirements. Furthermore, it should include the expenses for the subsequent five years, encompassing all licenses, hardware, subscriptions, and any additional costs related to maintaining and enhancing the proposed solution. This holistic approach ensures a transparent and accurate portrayal of the financial implications associated with the proposed solution over the specified duration.
- Bidder should consider that the above total workloads will be distributed among main and DR data centers depending on where active workload resides.
- The solution provider should consider the use of the existing VMware virtualization clusters at Hakeem datacenters (main and DR) to deploy the required servers within these clusters. The proposal must outline the specifications of virtual machines, including CPU, memory, storage, and network requirements, ensuring they align with availability, performance, scalability, and security criteria.
- In instances where the solution provider deems physical server deployment necessary, whether due to vendor mandates or specific performance demands or any backup or restore operations requiring the data stream to traverse the backup server, they should include the requisite physical servers in the proposal. These servers must be configured to meet availability, performance, scalability, and security requirements while seamlessly integrating with the existing infrastructure.
- Overall, the proposal should offer a comprehensive outline of the backup solution architecture, encompassing virtual or physical server

specifications, to satisfy Hakeem program availability, performance, scalability, and security requirements.

15. Lot (1): Technical Terms and Conditions - RMS

1. The bidder shall have at least two certified engineers according to the manufacturer's recommendations on the proposed solution; at least one of them shall be assigned to the project with EHS.
2. The bidder must be an authorized Partner of the mother company he represents in this bid; the highest two partnership levels are only accepted. The bidder must submit an up-to-date valid official letter/certificate from the mother company as part of the bidder's qualification documents.
3. The bidder shall have at least five enterprise scale live installations for similar solution. The references for such project must be provided within the proposal in order to be contacted by EHS as part of the technical evaluation.

16. Lot (1): Warranty and Support - RMS

1. The bidder shall offer minimum of (5) years (8/5) manufacturer warranty and support service. Vendor's support contract number / ID shall be provided to EHS.
2. The bidder shall offer minimum of (5) years (24/7) local maintenance and support service; Maintenance and support service shall cover all supplied components and services.
3. The Warranty and support services starting date is the date of the EHS's final acceptations of the completed scope of work.
4. During the warranty period, the supplier shall provide all required spare parts free of charge.
5. The warranty period covers support on site.
6. The bidder shall provide the support approach in the form of a signed and stamped SLA, including the escalation matrix, support contacts, and response time.
7. The bidder shall provide the yearly cost of the vendor's support service for additional one year, two years and five years after the five years of the product support end.
8. Perform preventive maintenance for the delivered solution based on four yearly visits during the warranty and support period.

17. Lot (1): License - RMS

1. Provide all the software and hardware licenses of any/all features that require purchasing a specific license to enable and use from day one. Further, describe how licenses are to be validated or enforced.
2. The bidder shall provide the required licenses to cover all the required capacity according to section “8 Bill of Quantity” from day one without under sizing.
3. All the licenses required for the solution must be perpetual licenses or for five years.
4. The vendor shall provide how solution licensing is deployed.
5. The supplier shall provide EHS the required licenses in the name of EHS to access and use the Software supplied through this RFP.

18. Lot (1): End-of-Life and End-of-Sale Conditions - RMS

1. The equipment quoted by the bidder should not be declared as End of Life (EOL) or End of Sale (EOS) by the manufacturer, at the time of bidding.
2. The bidder must provide a 5-year lifetime letter of the solution from the vendor.

19. Lot (1): Product origin - RMS

1. The mother company shall be from the USA, Europe, or Japan.
2. The Solution should be a Leader in Magic Quadrant for Enterprise Backup and Recovery Software Solutions

20. Lot (1): Technical Compliance Sheet - RMS

Description	Comply (Yes/No)
Business Requirements	
Backup and Recovery Software	
1. Data Source Compatibility: Ensure compatibility with diverse data sources, covering databases, virtual machines, containerized applications, applications, and file systems.	
2. Global Deduplication: Implement global deduplication to optimize storage utilization and reduce redundancy across data centers.	
3. Encryption: Provide end-to-end encryption for data in transit and at rest to meet security and compliance standards.	
4. Scalability: Scale seamlessly to accommodate the enterprise's growing data volumes and diverse workloads.	
Disaster Recovery Orchestration	
1. Automated Failover and Failback: Enable automated failover and failback procedures for quick and efficient disaster recovery.	
2. RTO and RPO Compliance: Ensure adherence to Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements According to ISO22301.	
3. Cross-Data Center Synchronization: Facilitate real-time or near-real-time synchronization between main and DR data centers.	
4. Testing and Validation: Allow for non-disruptive testing of disaster recovery plans that is related to ISO 22301 to validate their effectiveness.	
Cybersecurity Recovery:	
1. Air-Gapped Backups: Support air-gapped backups to create a physically isolated copy of critical data to protect against cyber threats.	
2. Immutable Backups: Implement immutability features to prevent unauthorized modifications to backup data.	
3. Incident Response Integration: Integrate with incident response systems (such as IBM security SOAR (Security Orchestration, Automation and Response, and others) to enhance the organization's ability to counter cybersecurity threats.	

4. Ransomware Detection and Mitigation: Provide advanced capabilities for ransomware detection, mitigation, and recovery.	

Compliance and Reporting:	
1. Audit Trails: Maintain comprehensive audit trails for backup, recovery, and disaster recovery operations.	
2. Regulatory Compliance: Ensure compliance with regulations and data protection laws.	
3. Customizable Reporting: Generate customizable reports on backup success, recovery points, and disaster recovery testing results.	
Management and Monitoring:	
1. Centralized Management Console: Offer a centralized console for configuring, monitoring, and managing backup and recovery operations.	
2. Alerting and Notifications: Provide real-time alerts and notifications for any anomalies, failures, or breaches.	
3. Role-Based Access Control: Implement role-based access controls to restrict access to sensitive backup and recovery functionalities.	
Integration and Compatibility:	
1. API Integration: Support APIs for seamless integration with other enterprise systems and workflows.	
2. Third-Party Integrations: Integrate with third-party tools and solutions for broader security and operational capabilities.	
Support and SLAs:	
1. 24/7 Technical Support: Ensure round-the-clock technical support for critical issues and emergencies.	
2. Service Level Agreements (SLAs): meet SLAs for backup, recovery, and disaster recovery timeframes according to the best practice and ISO 22301.	
Cost and Licensing:	
1. Transparent Pricing: Provide transparent pricing models with clear licensing terms and scalability options.	
2. Total Cost of Ownership (TCO): Consider the TCO, including hardware, software, and operational costs, for an accurate financial assessment.	

Description	Comply (Yes/No)
Solution Technical Specifications	
Backup and Recovery Software	
1. Comprehensive Backup and Recovery solution that provides flexible deployment options to ensure fast, secure backup and recovery for cloud, remote offices, and data center with client-side data deduplication.	
2. Solution should create application-consistent, image-level backups of Virtual Machines and Physical Servers, ensuring successful recovery of business-critical applications and services and allowing for application-specific restore scenarios.	
3. Solution must support backup of Windows and Linux physical servers, endpoints, containerized applications and Cloud VMs.	
4. Solution must support backup of entire image, volumes, or files or folders for physical servers and endpoints.	
5. Solution must provide the capability to protect Virtualized platform such as VMWare, Microsoft Hyper-V, Nutanix Acropolis Hypervisor (AHV) and Red Hat Virtualization (RHV) platforms using agentless mode.	
6. Solution should have the capability in divides backup data into variable-length sub-file segments, compresses and applies a unique hash identifier to each segment during the backup process.	
7. Solution must deduplicate data at the client, before transfer across the network.	
8. Solution must have the option to de-duplicate backup data at the target (if needed) for optimized efficiency with specific data types.	
9. Deduplication technology should dramatically reduce the amount of data sent and stored - eliminating backup bottlenecks and reducing storage costs	
10. Solution should determine if a segment has been previously backed up and only backs up the unique segments, greatly reducing backup times.	
11. Solution must have plugins/modules to integrate with most of third-party DB technologies as necessary.	
12. Solution must have a single pane of glass management software to simplify the prod and DR backup infrastructure management.	

13. Solution must provide the capability to backup VMWare workloads with zero stun-effect and no downtime during the backup process.	
14. Solution should provide a CDP (Continuous Data Protection) functionality to eliminate downtime and minimize data loss for Critical VMware vSphere workloads and perform immediate recoveries to a latest state or desired point in time achieving the most stringent RTO and RPO.	
15. Solution should provide end-to-end encryption for Server backup and replication data in flight and at rest.	
16. Must support granular restore of single email/file or other granular items directly from the de-duplicated storage on the appliance or repository without the need to duplicate or copy the backup to disk storage before restore	
17. Must Support self-service recovery natively for all Applications and VMware farm	
18. Solution should support VM configuration and Virtual Hard Disks restore.	
19. Solution should have an intelligent load-balancing of resources that allow parallel backup of VMs to reduce backup and replication windows	
20. Solution should automatically backup its configuration and it should provide a straightforward mechanism to restore the configuration in case of any failure.	
21. Solution should have the ability to instantly recover VMWare VM Guest OS files from backup with no need to deploy agents in production VMs or Hypervisor before backup.	
22. Solution should have the ability to view files from backups in the production Microsoft Windows file system and recover only the changed files.	
23. Solution must be able to deploy software agents on systems to be protected (no extra local hardware required, just license add in the future for specific applications & databases if required).	
24. Solution must reduce backup impact on client CPU.	
25. Solution should be able to recover individual application items (such as databases, e-mails, sites, users) from Microsoft Exchange, Active Directory, SQL, SharePoint, Oracle and PostgreSQL physical or virtual servers' backups.	
26. Solution should have an ability to instantly start VMware Virtual Machine directly from any backup disk storage at any chosen recovery point, on same or different virtualization host.	
27. Solution should have an ability to recover from an image-level backup including physical servers or workstations, virtual machines or cloud instances directly from any backup disk storage at any chosen recovery point to a VMWare vSphere, Hyper-V or AHV Virtual Machine.	

28. Solution should have the ability to instantly mount disks from any VMWare Virtual Machine backup to the selected VMware VM.	
29. Solution should include a Windows and Linux Guest OS file indexing feature and comprehensive OS file search engine in order to delegate file recovery operations to help desk or end users.	
30. Solution should support fast VM roll-back using Changed Block Tracking (CBT) restore and restore over SAN	
31. Solution should support file level, volume level, and bare-metal restore for Windows and Linux servers or workstations	
32. Solution should provide instant access to the content of any backup or replica to specialized third-party mining and security analysis applications and scripts that mounts the content of any restore point into the file system of the specified application server.	
33. Solution should provide automated backup verification technology for VMware vSphere, Virtual Machines and which will guarantee the recoverability of the Server at Guest OS and Application levels.	
34. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.	
35. Solution should perform an automated backup server configuration check against best practice guidelines to understand how backup infrastructures can be improved to address potential security concerns.	
36. Solution should be able to operate in modern data centers that are configured with IPv6 networking	
37. Solution should be able to track user actions and backup activities and gain complete transparency over file-level restore operations through specifically designed audit files	
38. Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.	
39. Solution should provide multi-tenant reporting and monitoring allowing multiple users to simultaneously access monitoring and reporting interfaces.	
40. Solution must be able to monitor storage datastore utilization and capacity planning / forecasting	
41. Solution should provide agentless data collection from virtualization hosts, management servers and failover clusters	
42. Solution should provide alerts and reports to identify and resolve common infrastructure and software misconfigurations before operational impact.	
43. Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.	

44. Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events	
45. Solution should support pre-defined reports and monitor location tags for VMs, hosts, computers configured in backup solution to observe data sovereignty.	
46. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks	
47. Must support multi-tenancy	

Description	Comply (Yes/No)
Purpose Built Backup Appliance	
1. Appliance Must be fully compatible with the proposed backup software and must support client direct backup from all servers and clients to the appliance without any need to add media agents	
2. Appliance Must provide an efficient, high performance inline deduplication technology with a local compression technique	
3. Deduplication process must utilize sub-file variable-length segment recognition and filtering process that works at block sizes as small as 4 kilobytes to maximize efficiency.	
4. The Storage Device shall be a self-contained disk system.	
5. Shall be able to support 16 or 32 Gbps FC connectivity for direct SAN connectivity if required in the future.	
6. Should include a minimum of two 10/25 Gbps Ethernet ports on separate network cards with 25 Gbps transceivers	
7. Should support Ethernet failover, Ethernet aggregation and VLAN tagging	
8. Appliance Must support an internal mechanism to provide the best defense against data integrity issues to continuously verify, detect and protect against data recoverability issues throughout the life cycle of the backup data	
9. Supports Distributed de-duplication processing using software Plugin on Backup Server	
10. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks	
11. Appliance Must Support WORM feature	
12. Appliance Must support Snapshot features to make read-only copy of the backup Images for protection	
13. Must provide high availability for all hardware components, such as power supplies, storage, and network interfaces. This minimizes the risk of a single point of failure.	
14. Dual disk parity RAID 6 with Spare or better technique	

15. Appliance should provide network-efficient, automated, ultra-safe replication for disaster recovery (DR), remote office data protection and multi-site consolidation.	
16. System must be capable of supporting replication/DR requirements such that deduplicated data starts replicating when backup starts to achieve faster Recovery Point Objectives	
17. Appliance Must support bi-directional, Many-to-One and cascaded replication between appliances	
18. Must support management of replication at backup software level	
19. Ability to access the backup images on the destination Appliance as read-only from backup servers	
20. Must support bandwidth throttling for replication	
21. Must have Web/Browser based Management GUI to manage multiple backup appliances from the same console	
22. Must support inline data-at-rest encryption	
23. Must support secure encrypted replication between appliances	
24. Must support Oracle Direct RMAN backup without the need to any backup Software	
25. The appliance must support Extended retentions capabilities for the long term archiving requirements	
26. The appliance must support direct backup to the cloud without any need to another Hardware in the middle between the appliance and the cloud storage	
27. The provided appliance shall support future increase in backup capacity to the double of the sizing space provided in this RFP	
28. The provided appliance shall provide Protection against NTP Attacks	
29. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.	
30. Must support multi-tenancy	
31. System must be capable of providing backup throughput of 25 TB/Hour	

Description	Comply (Yes/No)
Cybersecurity Recovery Solution	
1. Solution must provide isolated recovery backup copy that is totally physically isolated form the production network (air-gapped)	
2. Hardware and Software must be compatible with the provided Hardware and Software within the Data Protection Solution	
3. The solution must support creating multiple backup golden copies, by replicating a copy of backup data to a physically and logically isolated and protected vault. The golden copy must be scanned and verified.	
4. The replication between the existing backup and the isolated site must be automated and must use pull technique to pull the data from the main site	
5. Solution must support restore and validation workflow for the restored backup images	
6. Solution must be widely deployed and tested with enterprise customers	
7. Solution must support Air-gap technology	
8. Solution must provide Intelligent techniques to Analyze backed up data deep analysis from Meta Data , Header & Content	
9. Solution must provide machine learning and full-content indexing with powerful analytics within the safety of the vault.	
10. Solution must provide automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.	
11. Solution must create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production / backup environment and the vault.	
12. Solution must contain workflows and tools to perform recovery after an incident using dynamic restore processes and the existing DR procedure	
13. Solution must create an isolated environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance, The bidder shall provide all the required components for this isolated environment that are required to use and operate the solution according to vendor's recommendation.	
14. The provided solution shall provide protection against NTP Attacks	
15. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password	

credentials, to provide more secure access to the console and protect user accounts from being compromised.	
16. Must support Retention Lock capabilities for Archive requirements and to provide the best defense against ransomware attacks	
17. Solution Must support multi-tenancy	

Description	Comply (Yes/No)
Disaster Recovery, Replication and Orchestration Solution	
1. Solution should provide Service-level and Application-level monitoring and ensure the availability of mission-critical applications running in physical and virtual machines through enhanced, proactive application-level monitoring functionality, including the ability to track an individual application's health monitoring status as well as manage guest services and processes.	
2. Solution should offer reports covering all aspects of the Virtual Infrastructure; including VM availability (uptime), trend analysis, resource utilization, infrastructure documentation and management, and change tracking - for every object in the virtual infrastructure.	
3. Solution should present monitoring and reporting data from both technical and business-oriented perspectives. Business-oriented views are based on user-defined criteria and can include categorizations such as organizational structure, location, SLA, department, etc.	
4. Solution should be able to overlay event data on performance graphs for viewing the effect of events on utilization and trends	
5. Solution should provide visual status indicators on parent objects for at-a-glance notification of potential problems with underlying objects.	
6. Solution must automate recovery planning, testing and orchestrates the steps needed to recover from a planned or unplanned disaster	
7. Solution should create workflows to orchestrate recovery operations for both virtual and physical machines to VMware vSphere and public cloud environments	
8. Solution should be able to automate the verification of infrastructure readiness for recovery	
9. Solution must include Failover Orchestration allowing a 1-click failover for VMware VMs to avoid long downtimes.	
10. Solution must enable ability to include custom scripts to be executed in the orchestrated plan	
11. Solution must be able to verify the recovery plan automatically and upon schedule	
12. Solution must be able to automate recovery actions from backups	
13. Solution must be able to automate failover to VM replicas (Scheduled and CDP)	
14. Solution must be able to automate serving data from a destination or a secondary volume	
15. Solution should generate dynamic reports for orchestration plans that include a scope of orchestrated workloads, details	

on the recovery location, information on specific steps that will run during the recovery process, test execution details and summary information on plan test results	
16. Solution should support any point-in-time recovery to avoid logical corruption and roll back to any point in time	
17. Solution should support crash consistent and application consistent short term and long term replicas of virtual machines with near zero RPO	
18. Solution should provide the ability to group the virtual machines and applications into logical groups and stacks	
19. Solution should be able to orchestrate the recovery of virtual machines from backups and VM replicas in a defined order and with set customizable boot delays	
20. Solution should provide automated Replica verification technology for VMware vSphere Virtual Machines which will guarantee the failover of Virtual Machine at VM, Guest OS and Application levels	
21. Solution should provide an Intelligent VM Failover mechanism which includes Failover Plans, automated Re-IP, and network mapping of VMs on DR site and a failback technology which transfers only changed blocks back to production site.	
22. Solution should provide an option to execute custom scripts before and/or after the backup or VM replication jobs.	
23. Solution should provide Host based replication of EHS VMware vSphere Virtual Machines for High Availability and Disaster Recovery purposes managed from a single console.	
24. Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.	
25. Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events	
26. Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.	
27. Solution should have an intelligent load-balancing of resources that allow parallel Replication of VMs to reduce replication windows	
28. Solution must have the ability to facilitate large scale recovery by creating sophisticated DR plans and automatically executing them (i.e. application-specific steps)	
29. Solution should be able to create rich DR documentation, run test plans and verify application consistency	
30. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised	
31. Solution must support multi-tenancy	

Description	Comply (Yes/No)
Technical Terms and Conditions	
1. The bidder shall have at least two certified engineers according to the manufacturer's recommendations on the proposed solution; at least one of them shall be assigned to the project with EHS.	
2. The bidder must be an authorized Partner of the mother company he represents in this bid; the highest two partnership levels are only accepted. The bidder must submit an up-to-date valid official letter/certificate from the mother company as part of the bidder's qualification documents.	
3. The bidder shall have at least five enterprise scale live installations for similar solution. The references for such project must be provided within the proposal in order to be contacted by EHS as part of the technical evaluation.	

Description	Comply (Yes/No)
Warranty and Support	
1. The bidder shall offer minimum of (5) years (8/5) manufacturer warranty and support service. Vendor's support contract number / ID shall be provided to EHS.	
2. The bidder shall offer minimum of (5) years (24/7) local maintenance and support service; Maintenance and support service shall cover all supplied components and services.	
3. The Warranty and support services starting date is the date of the EHS's final acceptations of the completed scope of work.	
4. During the warranty period, the supplier shall provide all required spare parts free of charge.	
5. The warranty period covers support on site.	
6. The bidder shall provide the support approach in the form of a signed and stamped SLA, including the escalation matrix, support contacts, and response time.	
7. The bidder shall provide the yearly cost of the vendor's support service for additional one year, two years and five years after the five years of the product support end.	
8. Perform preventive maintenance for the delivered solution based on four yearly visits during the warranty and support period.	

Description	Comply (Yes/No)
License	
1. Provide the licenses of any/all features that require purchasing a specific license to enable and use. Further, describe how licenses are to be validated or enforced.	
2. All the licenses required for the solution must be perpetual licenses or for five years.	
3. The vendor shall provide how solution licensing is deployed.	
4. The supplier shall provide EHS the required licenses in the name of EHS to access and use the Software supplied through this RFP.	

Description	Comply (Yes/No)
End-of-Life and End-of-Sale Conditions	
1. The equipment quoted by the bidder should not be declared as End of Life (EOL) or End of Sale (EOS) by the manufacturer, at the time of bidding.	
2. The bidder must provide a 5-year lifetime letter of the solution from the vendor.	

Description	Comply (Yes/No)
Product origin	
1. The mother company shall be from the USA, Europe, or Japan.	
2. The Solution should be a Leader in Magic Quadrant for Enterprise Backup and Recovery Software Solutions	

21. Lot (1): Service Level Agreement - RMS

SLA Scope

The scope of this SLA agreement covers the provided solution for Backup and Data Protection Solution including all hardware and software components. On-site labor and parts must also be included.

SLA Duration

The supplier must provide maintenance and support for hardware and software for a period of five years starting the date of the EHS's final acceptations of the completed scope of work.

SLA Terms and conditions

The supplier response will be measured and monitored using EHS's Service Management tool.

During the Maintenance period, the supplier must provide the following:

- Preventive maintenance program and provide preventive maintenance scheduled visit every three months.
- Health check report after every preventive visit.
- Support methodology and escalation matrix including contacts details.
- Manufacturer support for all components.
- Maintaining spare parts to meet the "availability" target at no additional cost.
- Support, configure and resolve problems whenever needed and/or if requested by EHS.
- Commit to providing quality assurance for any major configuration changes whenever requested by EHS. Any change must be done within the EHS's Change Management process.
- Perform Firmware updates, patches, and new releases according to the manufacturer's recommendation
- Handle all support requests submitted within or outside working hours without extra charges.
- Provide the required assistance to EHS staff for any configuration modification.
- All the solution's components should be covered back-to-back by Vendor support without any exception; the supplier shall provide the approach to validate the support contract with the vendor to EHS.

Support Cases Management

EHS will set the support cases Severity level upon opening each individual support case.

Support cases covered by this agreement are to be treated by supplier according to the ITIL V4 framework incident management process and request fulfillment process, inline with the supplier provided support structure.

SLA Severity Levels and Targets

Severity Level 1: Critical

Definition:

This level represents incidents causing a critical impact to the business, resulting in severe disruption or complete unavailability of a critical system or service.

Examples:

- Complete system outage affecting all users.
- Security breach leading to unauthorized access to sensitive data.
- Data corruption or loss with significant business impact.

Response Time:

Immediate response required, typically within 1 hour.

Response Time Schedule:

24/7

Severity Level 2: High

Definition:

Incidents with high impact but not immediately critical, causing significant disruption or degradation in services.

Examples:

1. Major performance degradation affecting a critical business process.
2. Service interruptions affecting a specific department or location.
3. A security vulnerability that requires urgent attention.

Response Time:

Response within 2 hours.

Response Time Schedule:

24/7

Severity Level 3: Medium

Definition:

Incidents causing a moderate impact, resulting in disruption or degradation of non-critical services or affecting a limited number of users.

Examples:

- Performance issues affecting non-essential services.
- Application errors causing inconvenience but not critical to operations.
- Limited data loss with backups available for recovery.

Response Time:

Response within 4 hours.

Response Time Schedule:

Eight business-working hours - 5 Weekdays Excluding Holidays

Severity Level 4: Low

Definition:

Incidents causing minor impact, resulting in minimal disruption or inconvenience to users or business operations.

Examples:

- Minor performance issues with no critical impact.
- Non-urgent software or application bugs.
- Requests for information or non-urgent assistance.

Response Time:

Response within one business day.

Response Time Schedule:

Eight business-working hours - 5 Weekdays Excluding Holidays

During the resolution process of any problem, EHS team shall stay informed about the progress of the resolution process.

Following the completion of any service related to incident resolution (Severity Level 1 and Severity Level 2) and after closing the incident, the supplier shall provide an incident report. The Report shall include the Root Cause Analysis “RCA” and indicate the exact time at which an intervention began, the components that was serviced or replaced, the corrective measures that were taken, and the amount of time needed for the intervention since the manifestation of the problem until functionality is restored.

Response time: is the time it takes a provider to respond to an inquiry or request from a client.

SLA Availability Target and Penalties

Additional hours exceeding the allowable downtime will be subject to penalty. The minimum accepted system availability is 99.9% yearly uptime.

Throughout the execution of the SLA, vendors should not rely on system redundancy as a **permanent** resolution

The bidder will be subject to penalty if he does not meet the “response time”. The following table shows all the penalties under this SLA contract. In addition, the “response time” must be met with each Severity Level.

Penalty condition	Penalty amount per hour JoD			
	Severity Level 1	Severity Level 2	Severity Level 3	Severity Level 4
Failed to achieve 99.9% availability target	400	300	0	0
Failed to achieve "response time"	400	300	100	50

Availability: the ability of an IT system to perform its agreed function as required.

22. Lot (2): Business Requirements -MOH

From a business perspective, the new Data Protection Solution must be delivered as a robust, enterprise-grade turnkey solution meticulously tailored to align with EHS requirements and uphold industry standards for backup, data protection, disaster recovery orchestration, and cybersecurity recovery systems. This imperative encompasses a comprehensive approach addressing the following key points:

1. **Backup and Data Protection:**
    1) Data Source Compatibility: Ensure compatibility with diverse data sources, covering databases, virtual machines, containerized applications, applications, and file systems.
    2) Global Deduplication: Implement global deduplication to optimize storage utilization and reduce redundancy across data centers.
    3) Encryption: Provide end-to-end encryption for data in transit and at rest to meet security and compliance standards.
    4) Scalability: Scale seamlessly to accommodate the enterprise's growing data volumes and diverse workloads.

2. **Disaster Recovery Orchestration:**
    1) Automated Failover and Failback: Enable automated failover and failback procedures for quick and efficient disaster recovery.
    2) RTO and RPO Compliance: Ensure adherence to Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements According to ISO 22301.
    3) Cross-Data Center Synchronization: Facilitate real-time or near-real-time synchronization between main and DR data centers.
    4) Testing and Validation: Allow for non-disruptive testing of disaster recovery plans that is related to ISO 22301 to validate their effectiveness.

3. **Cybersecurity Recovery:**
    1) Air-Gapped Backups: Support air-gapped backups to create a physically isolated copy of critical data to protect against cyber threats.
       Immutable Backups: Implement immutability features to prevent unauthorized modifications to backup data.
    2) Incident Response Integration: Integrate with incident response systems (such as IBM security SOAR (Security Orchestration, Automation and Response, and others) to enhance the organization's ability to counter cybersecurity threats.
    3) Ransomware Detection and Mitigation: Provide advanced capabilities for ransomware detection, mitigation, and recovery.

4. **Compliance and Reporting:**
    1) Audit Trails: Maintain comprehensive audit trails for backup, recovery, and disaster recovery operations.
    2) Regulatory Compliance: Ensure compliance with regulations and data protection laws.
    3) Customizable Reporting: Generate customizable reports on backup success, recovery points, and disaster recovery testing results.

5. **Management and Monitoring:**
    1) Centralized Management Console: Offer a centralized console for configuring, monitoring, and managing backup and recovery operations.
    2) Alerting and Notifications: Provide real-time alerts and notifications for any anomalies, failures, or breaches.
    3) Role-Based Access Control: Implement role-based access controls to restrict access to sensitive backup and recovery functionalities.

6. **Integration and Compatibility:**
    1) API Integration: Support APIs for seamless integration with other enterprise systems and workflows.
    2) Third-Party Integrations: Integrate with third-party tools and solutions for broader security and operational capabilities.

7. **Support and SLAs:**
    1) 24/7 Technical Support: Ensure round-the-clock technical support for critical issues and emergencies.
    2) Service Level Agreements (SLAs): meet SLAs for backup, recovery, and disaster recovery timeframes according to the best practice and ISO 22301

8. **Cost and Licensing:**
    1) Transparent Pricing: Provide transparent pricing models with clear licensing terms and scalability options.
    2) Total Cost of Ownership (TCO): Consider the TCO, including hardware, software, and operational costs, for an accurate financial assessment.

23. Lot (2): Submittals -MOH

The bidders' proposal shall include the following:

1. Compliance sheets (for both technical and financial).
2. Data sheets for all items.
3. Project Implementation plan.
4. Accept Procedure Test (ATP) document.
5. Service level agreement (SLA)
6. Project team details.
7. Detailed BOQ (Item, QTY, and Duration)

24. Lot (2): RFP Objective -MOH

The objective of this RFP is to solicit proposals for the installation of an enterprise-level data protection solution in both the main and disaster recovery (DR) data centers. The selected solution should align seamlessly with our comprehensive business requirements, ensuring robust protection for databases, virtual machines, containerized applications, applications, and file systems.

The overarching objective is to identify a vendor capable of delivering a turnkey solution, expertly installed in both the main and DR data centers, ensuring the highest level of data protection, recovery, and resilience for EHS.

25. Lot (2): Solution Technical Specifications- MOH

25.1. Solution High-level Architecture

The proposed solution is envisaged to be seamlessly deployed across both Electronic Health Solutions (EHS) (Main) and Prince Hamzah Hospital (PHH) (DR) data centers, strategically addressing the imperative for High Availability (HA), Disaster Recovery (DR), and protect and recover against ransomware with threat protection capabilities. The prospective bidder is expected to intricately design and present a comprehensive solution architecture tailored to meet the unique demands of our main and DR data centers, while diligently accommodating the critical High Availability requirements.

This architecture should not only ensure the robust functioning of the system under normal operational conditions but also guarantee a swift and effective transition to the Disaster Recovery environment in the event of any unforeseen disruptions. Furthermore, the bidder's proposal should include a robust Cyber Recovery framework, incorporating best practices to safeguard critical data against cybersecurity threats. The proposed solution should outline a resilient framework that aligns seamlessly with the High Availability, Disaster Recovery and Cybersecurity Recovery mandates, ensuring the utmost protection and recoverability of our essential data assets.

During the project lifetime (minimum of five years), all the provided solution components and services (control and data planes) must resides within Hakeem program datacenters without the need to host / use any cloud based services or components.

For an effective data protection solution, it is best to get backup software, a backup appliance, and cybersecurity recovery from one vendor. This makes support simpler and ensures everything works smoothly together. A unified system reduces the chance of compatibility problems and is easier to manage. With one point of contact for support, issues get resolved faster, avoiding the complications of dealing with multiple vendors. This approach not only improves the reliability and performance of the data protection system but also makes it easier for users to manage and troubleshoot.

25.3. Backup and Data Protection Solution Technical Specifications [LOT One]

The Solution must offer effective capabilities to simplify management of data protection across complex enterprise environments. It must also ensure reliable recovery by protecting backup data against a constantly changing threat landscape, and expedite and orchestrate data recovery responses to traditional disaster and ransomware events. Below are the minimum technical specification for the solution:

25.2.1. Backup and Recovery Software

1) Comprehensive Backup and Recovery solution that provides flexible deployment options to ensure fast, secure backup and recovery for cloud, remote offices, and data center with client-side data deduplication.
2) Solution should create application-consistent, image-level backups of Virtual Machines and Physical Servers, ensuring successful recovery of business-critical applications and services and allowing for application-specific restore scenarios.
3) Solution must support backup of Windows and Linux physical servers, endpoints, containerized applications and Cloud VMs.
4) Solution must support backup of entire image, volumes, or files or folders for physical servers and endpoints.
5) Solution must provide the capability to protect Virtualized platform such as VMWare, Microsoft Hyper-V, Nutanix Acropolis Hypervisor (AHV) and Red Hat Virtualization (RHV) platforms using agentless mode.
6) Solution should have the capability in divides backup data into variable-length sub-file segments, compresses and applies a unique hash identifier to each segment during the backup process.
7) Solution must deduplicate data at the client, before transfer across the network.

8) Solution must have the option to de-duplicate backup data at the target (if needed) for optimized efficiency with specific data types.
9) Deduplication technology should dramatically reduce the amount of data sent and stored - eliminating backup bottlenecks and reducing storage costs
10) Solution should determine if a segment has been previously backed up and only backs up the unique segments, greatly reducing backup times.
11) Solution must have plugins/modules to integrate with most of third-party DB technologies as necessary.
12) Solution must have a single pane of glass management software to simplify the prod and DR backup infrastructure management.
13) Solution must provide the capability to backup VMWare workloads with zero stun-effect and no downtime during the backup process.
14) Solution should provide a CDP (Continuous Data Protection) functionality to eliminate downtime and minimize data loss for Critical VMware vSphere workloads and perform immediate recoveries to a latest state or desired point in time achieving the most stringent RTO and RPO.
15) Solution should provide end-to-end encryption for Server backup and replication data in flight and at rest.
16) Must support granular restore of single email/file or other granular items directly from the de-duplicated storage on the appliance or repository without the need to duplicate or copy the backup to disk storage before restore
17) Must Support self-service recovery natively for all Applications and VMware farm
18) Solution should support VM configuration and Virtual Hard Disks restore.
19) Solution should have an intelligent load-balancing of resources that allow parallel backup of VMs to reduce backup and replication windows
20) Solution should automatically backup its configuration and it should provide a straightforward mechanism to restore the configuration in case of any failure.
21) Solution should have the ability to instantly recover VMWare VM Guest OS files from backup with no need to deploy agents in production VMs or Hypervisor before backup.

22) Solution should have the ability to view files from backups in the production Microsoft Windows file system and recover only the changed files.
23) Solution must be able to deploy software agents on systems to be protected (no extra local hardware required, just license add in the future for specific applications & databases if required).
24) Solution must reduce backup impact on client CPU.
25) Solution should be able to recover individual application items (such as databases, e-mails, sites, users) from Microsoft Exchange, Active Directory, SQL, SharePoint, Oracle and PostgreSQL physical or virtual servers' backups.
26) Solution should have an ability to instantly start VMware Virtual Machine directly from any backup disk storage at any chosen recovery point, on same or different virtualization host.
27) Solution should have an ability to recover from an image-level backup including physical servers or workstations, virtual machines or cloud instances directly from any backup disk storage at any chosen recovery point to a VMWare vSphere, Hyper-V or AHV Virtual Machine.
28) Solution should have the ability to instantly mount disks from any VMWare Virtual Machine backup to the selected VMware VM.
29) Solution should include a Windows and Linux Guest OS file indexing feature and comprehensive OS file search engine in order to delegate file recovery operations to help desk or end users.
30) Solution should support fast VM roll-back using Changed Block Tracking (CBT) restore and restore over SAN
31) Solution should support file level, volume level, and bare-metal restore for Windows and Linux servers or workstations
32) Solution should provide instant access to the content of any backup or replica to specialized third-party mining and security analysis applications and scripts that mounts the content of any restore point into the file system of the specified application server.
33) Solution should provide automated backup verification technology for VMware vSphere, Virtual Machines and which will guarantee the recoverability of the Server at Guest OS and Application levels.
34) Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password

credentials, to provide more secure access to the console and protect user accounts from being compromised.

35) Solution should perform an automated backup server configuration check against best practice guidelines to understand how backup infrastructures can be improved to address potential security concerns.
36) Solution should be able to operate in modern data centers that are configured with IPv6 networking
37) Solution should be able to track user actions and backup activities and gain complete transparency over file-level restore operations through specifically designed audit files
38) Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.
39) Solution should provide multi-tenant reporting and monitoring allowing multiple users to simultaneously access monitoring and reporting interfaces.
40) Solution must be able to monitor storage datastore utilization and capacity planning / forecasting
41) Solution should provide agentless data collection from virtualization hosts, management servers and failover clusters
42) Solution should provide alerts and reports to identify and resolve common infrastructure and software misconfigurations before operational impact.
43) Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.
44) Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events
45) Solution should support pre-defined reports and monitor location tags for VMs, hosts, computers configured in backup solution to observe data sovereignty.
46) Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks
47) Solution should support multi-tenancy

25.2.2. Purpose Built Backup Appliance

1) Appliance Must be fully compatible with the proposed backup software and must support client direct backup from all

servers and clients to the appliance without any need to add media agents

2) Appliance Must provide an efficient, high performance inline deduplication technology with a local compression technique
3) Deduplication process must utilize sub-file variable-length segment recognition and filtering process that works at block sizes as small as 4 kilobytes to maximize efficiency.
4) The Storage Device shall be a self-contained disk system.
5) Shall be able to support 16 or 32 Gbps FC connectivity for direct SAN connectivity if required in the future.
6) Should include a minimum of two 10/25 Gbps Ethernet ports on separate network cards with 25 Gbps transceivers, including the transceivers from network switch side (Juniper EX4650)
7) Should support Ethernet failover, Ethernet aggregation and VLAN tagging
8) Appliance Must support an internal mechanism to provide the best defense against data integrity issues to continuously verify, detect and protect against data recoverability issues throughout the life cycle of the backup data
9) Supports Distributed de-duplication processing using software Plugin on Backup Server
10) Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks
11) Appliance Must Support WORM feature
12) Appliance Must support Snapshot features to make read-only copy of the backup Images for protection
13) Must provide high availability for all hardware components, such as power supplies, storage, and network interfaces. This minimizes the risk of a single point of failure.
14) Dual disk parity RAID 6 with Spare or better technique
15) Appliance should provide network-efficient, automated, ultra-safe replication for disaster recovery (DR), remote office data protection and multi-site consolidation.
16) System must be capable of supporting replication/DR requirements such that deduplicated data starts replicating when backup starts to achieve faster Recovery Point Objectives
17) Appliance Must support bi-directional, Many-to-One and cascaded replication between appliances

18) Must support management of replication at backup software level
19) Ability to access the backup images on the destination Appliance as read-only from backup servers
20) Must support bandwidth throttling for replication
21) Web/Browser based Management GUI to manage multiple backup appliances from the same console
22) Must support inline data-at-rest encryption
23) Must support secure encrypted replication between appliances
24) Must support Oracle Direct RMAN backup without the need to any backup Software
25) The appliance must support Extended retentions capabilities for the long term archiving requirements
26) The appliance must support direct backup to the cloud without any need to another Hardware in the middle between the appliance and the cloud storage
27) The provided appliance shall support future increase in backup capacity to the double of the sizing space provided in this RFP
28) The provided appliance shall provide Protection against NTP Attacks
29) Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.
30) Must support multi-tenancy
31) System must be capable of providing backup throughput of 25 TB/Hour

25.2.3. Cybersecurity Recovery Solution

1) Solution must provide isolated recovery backup copy that is totally physically isolated form the production network (air-gapped)
2) Hardware and Software must be compatible with the provided Hardware and Software within the Data Protection Solution
3) The solution must support creating multiple backup golden copies, by replicating a copy of backup data to a physically and logically isolated and protected vault. The golden copy must be scanned and verified.
4) The replication between the existing backup and the isolated site must be automated and must use pull technique to pull the data from the main site
5) Solution must support restore and validation workflow for the restored backup images
6) Solution must be widely deployed and tested with enterprise customers
7) Solution must support Air-gap technology
8) Solution must provide Intelligent techniques to Analyze backed up data deep analysis from Meta Data , Header & Content
9) Solution must provide machine learning and full-content indexing with powerful analytics within the safety of the vault.
10) Solution must provide automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.
11) Solution must create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production / backup environment and the vault.
12) Solution must contain workflows and tools to perform recovery after an incident using dynamic restore processes and the existing DR procedure
13) Solution must create an isolated environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance. The bidder shall provide all the required components for this isolated environment that are required to use and operate the solution according to vendor's best practice and complying with NIST SP 800-209 (Security Guidelines for Storage Infrastructure).
14) The provided solution shall provide protection against NTP Attacks
15) Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.
16) Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks
17) Solution Must support multi-tenancy

25.2.4. Disaster Recovery, Replication and Orchestration Solution

1) Solution should provide Service-level and Application-level monitoring and ensure the availability of mission-critical applications running in physical and virtual machines through enhanced, proactive application-level monitoring functionality, including the ability to track an individual application's health monitoring status as well as manage guest services and processes.
2) Solution should offer reports covering all aspects of the Virtual Infrastructure; including VM availability (uptime), trend analysis, resource utilization, infrastructure documentation and management, and change tracking - for every object in the virtual infrastructure.
3) Solution should present monitoring and reporting data from both technical and business-oriented perspectives. Business-oriented views are based on user-defined criteria and can include categorizations such as organizational structure, location, SLA, department, etc.
4) Solution should be able to overlay event data on performance graphs for viewing the effect of events on utilization and trends
5) Solution should provide visual status indicators on parent objects for at-a-glance notification of potential problems with underlying objects.
6) Solution must automate recovery planning, testing and orchestrates the steps needed to recover from a planned or unplanned disaster
7) Solution should create workflows to orchestrate recovery operations for both virtual and physical machines to VMware vSphere and public cloud environments
8) Solution should be able to automate the verification of infrastructure readiness for recovery
9) Solution must include Failover Orchestration allowing a 1-click failover for VMware VMs to avoid long downtimes.
10) Solution must enable ability to include custom scripts to be executed in the orchestrated plan
11) Solution must be able to verify the recovery plan automatically and upon schedule
12) Solution must be able to automate recovery actions from backups
13) Solution must be able to automate failover to VM replicas (Scheduled and CDP)
14) Solution must be able to automate serving data from a destination or a secondary volume

15) Solution should generate dynamic reports for orchestration plans that include a scope of orchestrated workloads, details on the recovery location, information on specific steps that will run during the recovery process, test execution details and summary information on plan test results
16) Solution should support any point-in-time recovery to avoid logical corruption and roll back to any point in time
17) Solution should support crash consistent and application consistent short term and long term replicas of virtual machines with near zero RPO
18) Solution should provide the ability to group the virtual machines and applications into logical groups and stacks
19) Solution should be able to orchestrate the recovery of virtual machines from backups and VM replicas in a defined order and with set customizable boot delays
20) Solution should provide automated Replica verification technology for VMware vSphere Virtual Machines which will guarantee the failover of Virtual Machine at VM, Guest OS and Application levels
21) Solution should provide an Intelligent VM Failover mechanism which includes Failover Plans, automated Re-IP, and network mapping of VMs on DR site and a failback technology which transfers only changed blocks back to production site.
22) Solution should provide an option to execute custom scripts before and/or after the backup or VM replication jobs.
23) Solution should provide Host based replication of EHS VMware vSphere Virtual Machines for High Availability and Disaster Recovery purposes managed from a single console.
24) Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.
25) Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events
26) Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.
27) Solution should have an intelligent load-balancing of resources that allow parallel Replication of VMs to reduce replication windows
28) Solution must have the ability to facilitate large scale recovery by creating sophisticated DR plans and automatically executing them (i.e. application-specific steps)
29) Solution should be able to create rich DR documentation, run test plans and verify application consistency

30) Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised
31) Solution must support multi-tenancy

25.3. Microsoft Office 365 Backup Solution [LOT TWO]

The primary goal of this solution is to provide a creative and comprehensive solution that will supply EHS with a reliable backup and recovery solution for our Office 365 Exchange Online, SharePoint Online, OneDrive and Microsoft Teams platforms. Office 365 External backup solution should include unlimited retention space and an unrestricted retention policy. Office 365 data must remain fully backed up and recoverable at all times.

The solution shall be licensed based on number of the active users. Currently EHS has around 300+ users.

The following are the minimum requirements for the intended solution:

- Recovery model that includes:
    - Granular recovery of SharePoint, OneDrive and Teams documents
    - Individual and mass restore and recovery of Exchange mailboxes
- Unlimited retention included
- Scalable as our organization grows
- 100% cloud based
- All restore operations must be nondestructive, and not overwrite existing data
- Ability to restore from a former users' account
- Ability to perform backups on Exchange Online, OneDrive, SharePoint, and Teams
- Find and recover the data quickly and easily with advanced search functionalities via dashboard
- Only required to license current employees while still maintaining data from past employees.
- Provide ongoing maintenance and technical support throughout the duration of the Contract

26. Lot (2): Scope of Work - MOH

The scope for delivering the Backup and Data Protection Solution shall include the following:

1) **Project Kickoff:**

   a. Hold an initial meeting to align project objectives and timelines.
   b. Define roles and responsibilities.
   c. Develop a Project implementation plan and project schedule. The supplier shall assign a qualified technical project manager to manage the project and to ensure the controls and successful delivery.

2) **Solution Components Delivery**

   a. The delivery of all the solution components to EHS Warehouse and the sites based on EHS requirements and policies, including moving the materials to and within the sites.

3) **Pre-Implementation Assessment:**

   a. Perform preparatory site visits and related activities to ensure the best deployment.
   b. Conduct an assessment of the existing IT infrastructure.
   c. Identify specific requirements and constraints.

4) **Solution Design:**

   a. Develop a detailed solution design based on the provided business requirements.
   b. Include architecture diagrams, component specifications, and integration points.
   c. Conduct technical workshops with EHS technical team to develop the solution architecture, HLD, and LLD. The entire project's documentation must be approved by EHS.
   d. The solution design must be provided by the vendor end-to-end

5) **Solution Setup and Installation:**

   a. Deploy necessary hardware and software components.
   b. Configure solution's equipment.

c. Follow EHS instructions in labeling all equipment and switches and put a description in the network devices configuration.
d. Patching the copper and fiber patch cords cables inside the cabinets.
e. Provide any extra materials or/and services required to deliver a complete turnkey solution.

6) **Integration and Compatibility:**

a. Ensure seamless integration with existing enterprise systems.
b. Verify compatibility with databases, virtual machines, containerized applications, and other data sources.

7) **Configuration and Optimization:**

a. Configure backup software to meet EHS full requirements that are compliant with ISO27001, including but not limited to: backup policies, schedules, and retention periods.
b. Optimize performance for scalability and efficiency.
c. Establish disaster recovery configurations for main and DR data centers.
d. Define failover and failback procedures.
e. The vendor shall provide the full implementation, configuration and testing for the Cybersecurity Recovery Solution.

8) **Security Measures:**

a. Implement end-to-end encryption for data in transit and at rest without any additional components from EHS
b. Set up access controls and authentication mechanisms according to EHS policies

9) **Testing and Validation:**

a. Conduct thorough testing of backup and recovery processes.
b. Validate disaster recovery plans through simulated scenarios.
c. Perform Acceptance Test Procedure (onsite) and any corrective action to collect EHS acceptance.
d. The vendor must provide the final validation for the implemented solution.

10) **User Training:**

a. Develop training materials for operator and IT administration staff.
b. Provide training sessions to ensure proper utilization of the data protection solution.

11) **Documentation:**

a. Document the implemented solution comprehensively.
b. Include configuration guides, operational manuals, and troubleshooting procedures.

12) **Monitoring and Alerting:**

a. Set up monitoring tools to track the health and performance of the data protection system.
b. Configure alerting mechanisms for immediate issue detection.

13) **Reporting:**

a. Implement customizable reporting features.
b. Generate reports on backup success, recovery points, and disaster recovery testing results.

14) **Knowledge Transfer:**

a. Transfer knowledge to the IT team for ongoing system management.
b. Provide guidance on routine maintenance tasks.

15) **Post-Implementation Support:**

a. Offer post-implementation support to address any issues or concerns.
b. Conduct periodic reviews to ensure optimal system performance.

27. Lot (2): Deliverables -MOH

1) **Detailed Solution Design Document:**

a. Architecture diagrams.
b. Component specifications.

2) **Configured Solution:**

a. Deployed and configured hardware and software components.

3) **Integration Documentation:**

a. Documentation on integration with existing systems.

4) **Backup and Data Protection Policies:**

a. Configured backup policies, schedules, and retention periods.

5) **Security Documentation:**

   a. Documentation on implemented cybersecurity measures.

6) **Disaster Recovery Plans:**

   a. Detailed disaster recovery plans for main and DR data centers.

7) **Testing Reports:**

   a. Reports on testing and validation activities.

8) **User Training Materials:**

   a. Training materials for end-users and IT staff.

9) Comprehensive Documentation:

   a. Operational manuals, configuration guides, and troubleshooting procedures.

10) **Monitoring and Alerting Setup:**

   a. Configured monitoring tools and alerting mechanisms.

11) **Reporting Templates:**

   a. Templates for customizable reports.

12) **Knowledge Transfer Session Records:**

   a. Records of knowledge transfer sessions.

13) **Post-Implementation Support Agreement:**

   a. Formal agreement for post-implementation support. Provide the support approach in the form of signed and stamped SLA, including the escalation matrix, support contacts and response time.

28. Lot (2): Bill of Quantities -MOH

The below is the BOQ for the solution included in the below table, each components sizing and license requirement is based on the below details within this section.

Item	Location	Description	Qty
1	Main Datacenter	Backup and Recovery Software	1
2	DR Datacenter	Backup and Recovery Software	1
3	Main Datacenter	Disaster Recovery and Replication Solution	1
4	DR Datacenter	Disaster Recovery and Replication Solution	1
5	Main Datacenter	Purpose Built Backup Appliance	1
6	DR Datacenter	Purpose Built Backup Appliance	1
7	Main Datacenter	Cybersecurity Recovery Solution	1

The solution sizing and capacity shall be based on the following criteria as minimum; these criteria are required for providing the needed licenses, hardware performance, and storage capacity

#	Workload	Data Growth Yearly	Daily Change	Size TB	QTY	Backup Policy
1	Virtual Machines - DB	10%	3%	7	90	5. Daily Incremental with 1 Week Retention 6. Weekly Full with 4 Weeks Retention 7. Monthly Full with 12 Months retention 8. Yearly Full with 1 Year Retention
2	Virtual Machines – File System	15%	3%	18	10	
3	Physical Server -	15%	3%	3	1	

	Exchange Server					
4	Virtual Machines - Kubernetes / Rancher	10%	3%	1	3	
5	Physical Server - Oracle Database	10%	3%	1	1	
6	Physical Server - Generic DBs	15%	3%	5	1	

- Kubernetes / Rancher platform is intended to run 20 applications
- Cybersecurity Recovery Solution to be isolated in different Purpose Built Backup Appliance with deep analysis based on technical requirements in “Cybersecurity Recovery Solution” section.
- Backup and Recovery Solution to cover all workloads mentioned above. In addition, based on the architecture described in the “Solution High-level Architecture” section.
- The bidding entity is required to furnish a comprehensive analysis of the total cost of ownership for the proposed solution delineated in this RFP. This entails presenting a detailed breakdown of the total solution cost over a ten-year span, distinctly outlined in the financial offer's separate section. The cumulative total cost of ownership should encompass the initial expenses associated with the solution, as stipulated by the RFP requirements. Furthermore, it should include the expenses for the subsequent five years, encompassing all necessary licenses, hardware, subscriptions, and any additional costs related to maintaining and enhancing the proposed solution. This holistic approach ensures a transparent and accurate portrayal of the financial implications associated with the proposed solution over the specified duration.
- Bidder should consider that the above total workloads will be distributed among main and DR data centers depending on where active virtual machine resides.
- The solution provider should consider the use of the existing VMware virtualization clusters at Hakeem datacenters (main and DR) to deploy the required servers within these clusters. The proposal must outline the specifications of virtual machines, including CPU, memory, storage, and

network requirements, ensuring they align with availability, performance, scalability, and security criteria.

- In instances where the solution provider deems physical server deployment necessary, whether due to vendor mandates or specific performance demands or any backup or restore operations requiring the data stream to traverse the backup server, they should include the requisite physical servers in the proposal. These servers must be configured to meet availability, performance, scalability, and security requirements while seamlessly integrating with the existing infrastructure.
- Overall, the proposal should offer a comprehensive outline of the backup solution architecture, encompassing virtual or physical server specifications, to satisfy Hakeem program availability, performance, scalability, and security requirements.
- The bidder shall provide their proposals for office 365 backup solution as separate sections in the technical and financial proposal considering that EHS has a plan to migrate to MS office 365 in the near future, the number of MS Office users is around 300 users.

29. Lot (2): Technical Terms and Conditions - MOH

1. The bidder shall have at least two certified engineers according to the manufacturer's recommendations on the proposed solution; at least one of them shall be assigned to the project with EHS.
2. The bidder must be an authorized Partner of the mother company he represents in this bid; the highest two partnership levels are only accepted. The bidder must submit an up-to-date valid official letter/certificate from the mother company as part of the bidder's qualification documents.
3. The bidder shall have at least five enterprise scale live installations for similar solution. The references for such project must be provided within the proposal in order to be contacted by EHS as part of the technical evaluation.

30. Lot (2): Warranty and Support - MOH

1. The bidder shall offer minimum of (5) years (8/5) manufacturer warranty and support service. Vendor's support contract number / ID shall be provided to EHS.
2. The bidder shall offer minimum of (5) years (24/7) local maintenance and support service; Maintenance and support service shall cover all supplied components and services.
3. The Warranty and support services starting date is the date of the EHS's final acceptations of the completed scope of work.
4. During the warranty period, the supplier shall provide all required spare parts free of charge.
5. The warranty period covers support on site.

6. The bidder shall provide the support approach in the form of a signed and stamped SLA, including the escalation matrix, support contacts, and response time.
7. The bidder shall provide the yearly cost of the vendor's support service for additional one year, two years and five years after the five years of the product support end.
8. Perform preventive maintenance for the delivered solution based on four yearly visits during the warranty and support period.

31. Lot (2): License - MOH

1. Provide all the software and hardware licenses of any/all features that require purchasing a specific license to enable and use from day one. Further, describe how licenses are to be validated or enforced.
2. The bidder shall provide the required licenses to cover all the required capacity according to section “8 Bill of Quantity” from day one without under sizing.
3. All the licenses required for the solution must be perpetual licenses or for five years.
4. The vendor shall provide how solution licensing is deployed.
5. The supplier shall provide EHS the required licenses in the name of EHS to access and use the Software supplied through this RFP.

32. Lot (2): End-of-Life and End-of-Sale Conditions - MOH

1. The equipment quoted by the bidder should not be declared as End of Life (EOL) or End of Sale (EOS) by the manufacturer, at the time of bidding.
2. The bidder must provide a 5-year lifetime letter of the solution from the vendor.

33. Lot (2): Product origin - MOH

1. The mother company shall be from the USA, Europe, or Japan.
2. The Solution should be a Leader in Magic Quadrant for Enterprise Backup and Recovery Software Solutions

34. Lot (2): Technical Compliance Sheet - MOH

Description	Comply (Yes/No)
Business Requirements	
Backup and Recovery Software	
1. Data Source Compatibility: Ensure compatibility with diverse data sources, covering databases, virtual machines, containerized applications, applications, and file systems.	
2. Global Deduplication: Implement global deduplication to optimize storage utilization and reduce redundancy across data centers.	
3. Encryption: Provide end-to-end encryption for data in transit and at rest to meet security and compliance standards.	
4. Scalability: Scale seamlessly to accommodate the enterprise's growing data volumes and diverse workloads.	
Disaster Recovery Orchestration	
1. Automated Failover and Failback: Enable automated failover and failback procedures for quick and efficient disaster recovery.	
2. RTO and RPO Compliance: Ensure adherence to Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements According to ISO22301.	
3. Cross-Data Center Synchronization: Facilitate real-time or near-real-time synchronization between main and DR data centers.	
4. Testing and Validation: Allow for non-disruptive testing of disaster recovery plans that is related to ISO 22301 to validate their effectiveness.	
Cybersecurity Recovery:	
1. Air-Gapped Backups: Support air-gapped backups to create a physically isolated copy of critical data to protect against cyber threats.	
2. Immutable Backups: Implement immutability features to prevent unauthorized modifications to backup data.	
3. Incident Response Integration: Integrate with incident response systems (such as IBM security SOAR (Security Orchestration, Automation and Response, and others) to enhance the organization's ability to counter cybersecurity threats.	

4. Ransomware Detection and Mitigation: Provide advanced capabilities for ransomware detection, mitigation, and recovery.	

Compliance and Reporting:	
1. Audit Trails: Maintain comprehensive audit trails for backup, recovery, and disaster recovery operations.	
2. Regulatory Compliance: Ensure compliance with regulations and data protection laws.	
3. Customizable Reporting: Generate customizable reports on backup success, recovery points, and disaster recovery testing results.	
Management and Monitoring:	
1. Centralized Management Console: Offer a centralized console for configuring, monitoring, and managing backup and recovery operations.	
2. Alerting and Notifications: Provide real-time alerts and notifications for any anomalies, failures, or breaches.	
3. Role-Based Access Control: Implement role-based access controls to restrict access to sensitive backup and recovery functionalities.	
Integration and Compatibility:	
1. API Integration: Support APIs for seamless integration with other enterprise systems and workflows.	
2. Third-Party Integrations: Integrate with third-party tools and solutions for broader security and operational capabilities.	
Support and SLAs:	
1. 24/7 Technical Support: Ensure round-the-clock technical support for critical issues and emergencies.	
2. Service Level Agreements (SLAs): meet SLAs for backup, recovery, and disaster recovery timeframes according to the best practice and ISO 22301.	
Cost and Licensing:	
1. Transparent Pricing: Provide transparent pricing models with clear licensing terms and scalability options.	
2. Total Cost of Ownership (TCO): Consider the TCO, including hardware, software, and operational costs, for an accurate financial assessment.	

Description	Comply (Yes/No)
Solution Technical Specifications	
Backup and Recovery Software	
1. Comprehensive Backup and Recovery solution that provides flexible deployment options to ensure fast, secure backup and recovery for cloud, remote offices, and data center with client-side data deduplication.	
2. Solution should create application-consistent, image-level backups of Virtual Machines and Physical Servers, ensuring successful recovery of business-critical applications and services and allowing for application-specific restore scenarios.	
3. Solution must support backup of Windows and Linux physical servers, endpoints, containerized applications and Cloud VMs.	
4. Solution must support backup of entire image, volumes, or files or folders for physical servers and endpoints.	
5. Solution must provide the capability to protect Virtualized platform such as VMWare, Microsoft Hyper-V, Nutanix Acropolis Hypervisor (AHV) and Red Hat Virtualization (RHV) platforms using agentless mode.	
6. Solution should have the capability in divides backup data into variable-length sub-file segments, compresses and applies a unique hash identifier to each segment during the backup process.	
7. Solution must deduplicate data at the client, before transfer across the network.	
8. Solution must have the option to de-duplicate backup data at the target (if needed) for optimized efficiency with specific data types.	
9. Deduplication technology should dramatically reduce the amount of data sent and stored - eliminating backup bottlenecks and reducing storage costs	
10. Solution should determine if a segment has been previously backed up and only backs up the unique segments, greatly reducing backup times.	
11. Solution must have plugins/modules to integrate with most of third-party DB technologies as necessary.	
12. Solution must have a single pane of glass management software to simplify the prod and DR backup infrastructure management.	
13. Solution must provide the capability to backup VMWare workloads with zero stun-effect and no downtime during the backup process.	

14. Solution should provide a CDP (Continuous Data Protection) functionality to eliminate downtime and minimize data loss for Critical VMware vSphere workloads and perform immediate recoveries to a latest state or desired point in time achieving the most stringent RTO and RPO.	
15. Solution should provide end-to-end encryption for Server backup and replication data in flight and at rest.	
16. Must support granular restore of single email/file or other granular items directly from the de-duplicated storage on the appliance or repository without the need to duplicate or copy the backup to disk storage before restore	
17. Must Support self-service recovery natively for all Applications and VMware farm	
18. Solution should support VM configuration and Virtual Hard Disks restore.	
19. Solution should have an intelligent load-balancing of resources that allow parallel backup of VMs to reduce backup and replication windows	
20. Solution should automatically backup its configuration and it should provide a straightforward mechanism to restore the configuration in case of any failure.	
21. Solution should have the ability to instantly recover VMWare VM Guest OS files from backup with no need to deploy agents in production VMs or Hypervisor before backup.	
22. Solution should have the ability to view files from backups in the production Microsoft Windows file system and recover only the changed files.	
23. Solution must be able to deploy software agents on systems to be protected (no extra local hardware required, just license add in the future for specific applications & databases if required).	
24. Solution must reduce backup impact on client CPU.	
25. Solution should be able to recover individual application items (such as databases, e-mails, sites, users) from Microsoft Exchange, Active Directory, SQL, SharePoint, Oracle and PostgreSQL physical or virtual servers' backups.	
26. Solution should have an ability to instantly start VMware Virtual Machine directly from any backup disk storage at any chosen recovery point, on same or different virtualization host.	
27. Solution should have an ability to recover from an image-level backup including physical servers or workstations, virtual machines or cloud instances directly from any backup disk storage at any chosen recovery point to a VMWare vSphere, Hyper-V or AHV Virtual Machine.	

28. Solution should have the ability to instantly mount disks from any VMWare Virtual Machine backup to the selected VMware VM.	
29. Solution should include a Windows and Linux Guest OS file indexing feature and comprehensive OS file search engine in order to delegate file recovery operations to help desk or end users.	
30. Solution should support fast VM roll-back using Changed Block Tracking (CBT) restore and restore over SAN	
31. Solution should support file level, volume level, and bare-metal restore for Windows and Linux servers or workstations	
32. Solution should provide instant access to the content of any backup or replica to specialized third-party mining and security analysis applications and scripts that mounts the content of any restore point into the file system of the specified application server.	
33. Solution should provide automated backup verification technology for VMware vSphere, Virtual Machines and which will guarantee the recoverability of the Server at Guest OS and Application levels.	
34. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.	
35. Solution should perform an automated backup server configuration check against best practice guidelines to understand how backup infrastructures can be improved to address potential security concerns.	
36. Solution should be able to operate in modern data centers that are configured with IPv6 networking	
37. Solution should be able to track user actions and backup activities and gain complete transparency over file-level restore operations through specifically designed audit files	
38. Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.	
39. Solution should provide multi-tenant reporting and monitoring allowing multiple users to simultaneously access monitoring and reporting interfaces.	
40. Solution must be able to monitor storage datastore utilization and capacity planning / forecasting	
41. Solution should provide agentless data collection from virtualization hosts, management servers and failover clusters	

42. Solution should provide alerts and reports to identify and resolve common infrastructure and software misconfigurations before operational impact.	
43. Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.	
44. Solution should provide alarm customization and modeling against past performance data to understand potential alarm frequency and avoid inadvertent alert storms and missed events	
45. Solution should support pre-defined reports and monitor location tags for VMs, hosts, computers configured in backup solution to observe data sovereignty.	
46. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks	
47. Must support multi-tenancy	

Description	Comply (Yes/No)
Purpose Built Backup Appliance	
1. Appliance Must be fully compatible with the proposed backup software and must support client direct backup from all servers and clients to the appliance without any need to add media agents	
2. Appliance Must provide an efficient, high performance inline deduplication technology with a local compression technique	
3. Deduplication process must utilize sub-file variable-length segment recognition and filtering process that works at block sizes as small as 4 kilobytes to maximize efficiency.	
4. The Storage Device shall be a self-contained disk system.	
5. Shall be able to support 16 or 32 Gbps FC connectivity for direct SAN connectivity if required in the future.	
6. Should include a minimum of two 10/25 Gbps Ethernet ports on separate network cards with 25 Gbps transceivers	
7. Should support Ethernet failover, Ethernet aggregation and VLAN tagging	
8. Appliance Must support an internal mechanism to provide the best defense against data integrity issues to continuously verify, detect and protect against data recoverability issues throughout the life cycle of the backup data	
9. Supports Distributed de-duplication processing using software Plugin on Backup Server	
10. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks	

11. Appliance Must Support WORM feature	
12. Appliance Must support Snapshot features to make read-only copy of the backup Images for protection	
13. Must provide high availability for all hardware components, such as power supplies, storage, and network interfaces. This minimizes the risk of a single point of failure.	
14. Dual disk parity RAID 6 with Spare or better technique	
15. Appliance should provide network-efficient, automated, ultra-safe replication for disaster recovery (DR), remote office data protection and multi-site consolidation.	
16. System must be capable of supporting replication/DR requirements such that deduplicated data starts replicating when backup starts to achieve faster Recovery Point Objectives	
17. Appliance Must support bi-directional, Many-to-One and cascaded replication between appliances	
18. Must support management of replication at backup software level	
19. Ability to access the backup images on the destination Appliance as read-only from backup servers	
20. Must support bandwidth throttling for replication	
21. Web/Browser based Management GUI to manage multiple backup appliances from the same console	
22. Must support inline data-at-rest encryption	
23. Must support secure encrypted replication between appliances	
24. Must support Oracle Direct RMAN backup without the need to any backup Software	
25. The appliance must support Extended retentions capabilities for the long term archiving requirements	
26. The appliance must support direct backup to the cloud without any need to another Hardware in the middle between the appliance and the cloud storage	
27. The provided appliance shall support future increase in backup capacity to the double of the sizing space provided in this RFP	
28. The provided appliance shall provide Protection against NTP Attacks	
29. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.	
30. Must support multi-tenancy	
31. System must be capable of providing backup throughput of 25 TB/Hour	

Description	Comply (Yes/No)
Cybersecurity Recovery Solution	
1. Solution must provide isolated recovery backup copy that is totally physically isolated form the production network (air-gapped)	
2. Hardware and Software must be compatible with the provided Hardware and Software within the Data Protection Solution	
3. The solution must support creating multiple backup golden copies, by replicating a copy of backup data to a physically and logically isolated and protected vault. The golden copy must be scanned and verified.	
4. The replication between the existing backup and the isolated site must be automated and must use pull technique to pull the data from the main site	
5. Solution must support restore and validation workflow for the restored backup images	
6. Solution must be widely deployed and tested with enterprise customers	
7. Solution must support Air-gap technology	
8. Solution must provide Intelligent techniques to Analyze backed up data deep analysis from Meta Data , Header & Content	
9. Solution must provide machine learning and full-content indexing with powerful analytics within the safety of the vault.	
10. Solution must provide automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.	
11. Solution must create unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production / backup environment and the vault.	
12. Solution must contain workflows and tools to perform recovery after an incident using dynamic restore processes and the existing DR procedure	
13. Solution must create an isolated environment that is disconnected from corporate and backup networks and restricted from users other than those with proper clearance, The bidder shall provide all the required components for this isolated environment that are required to use and operate the solution according to vendor's recommendation.	

14. The provided solution shall provide protection against NTP Attacks	
15. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised.	
16. Must support Retention Lock capabilities for Archive requirement and to provide the best defense against ransomware attacks	
17. Solution must support multi-tenancy	

Description	Comply (Yes/No)
Disaster Recovery, Replication and Orchestration Solution	
1. Solution should provide Service-level and Application-level monitoring and ensure the availability of mission-critical applications running in physical and virtual machines through enhanced, proactive application-level monitoring functionality, including the ability to track an individual application's health monitoring status as well as manage guest services and processes.	
2. Solution should offer reports covering all aspects of the Virtual Infrastructure; including VM availability (uptime), trend analysis, resource utilization, infrastructure documentation and management, and change tracking - for every object in the virtual infrastructure.	
3. Solution should present monitoring and reporting data from both technical and business-oriented perspectives. Business-oriented views are based on user-defined criteria and can include categorizations such as organizational structure, location, SLA, department, etc.	
4. Solution should be able to overlay event data on performance graphs for viewing the effect of events on utilization and trends	
5. Solution should provide visual status indicators on parent objects for at-a-glance notification of potential problems with underlying objects.	
6. Solution must automate recovery planning, testing and orchestrates the steps needed to recover from a planned or unplanned disaster	
7. Solution should create workflows to orchestrate recovery operations for both virtual and physical machines to VMware vSphere and public cloud environments	
8. Solution should be able to automate the verification of infrastructure readiness for recovery	

9. Solution must include Failover Orchestration allowing a 1-click failover for VMware VMs to avoid long downtimes.	
10. Solution must enable ability to include custom scripts to be executed in the orchestrated plan	
11. Solution must be able to verify the recovery plan automatically and upon schedule	
12. Solution must be able to automate recovery actions from backups	
13. Solution must be able to automate failover to VM replicas (Scheduled and CDP)	
14. Solution must be able to automate serving data from a destination or a secondary volume	
15. Solution should generate dynamic reports for orchestration plans that include a scope of orchestrated workloads, details on the recovery location, information on specific steps that will run during the recovery process, test execution details and summary information on plan test results	
16. Solution should support any point-in-time recovery to avoid logical corruption and roll back to any point in time	
17. Solution should support crash consistent and application consistent short term and long term replicas of virtual machines with near zero RPO	
18. Solution should provide the ability to group the virtual machines and applications into logical groups and stacks	
19. Solution should be able to orchestrate the recovery of virtual machines from backups and VM replicas in a defined order and with set customizable boot delays	
20. Solution should provide automated Replica verification technology for VMware vSphere Virtual Machines which will guarantee the failover of Virtual Machine at VM, Guest OS and Application levels	
21. Solution should provide an Intelligent VM Failover mechanism which includes Failover Plans, automated Re-IP, and network mapping of VMs on DR site and a failback technology which transfers only changed blocks back to production site.	
22. Solution should provide an option to execute custom scripts before and/or after the backup or VM replication jobs.	
23. Solution should provide Host based replication of EHS VMware vSphere Virtual Machines for High Availability and Disaster Recovery purposes managed from a single console.	
24. Solution should provide automated report generation and delivery to mailboxes, dashboards, web portals or archives.	
25. Solution should provide alarm customization and modeling against past performance data to understand potential	

alarm frequency and avoid inadvertent alert storms and missed events	
26. Solution must allow multiple users to simultaneously access monitoring and reporting interfaces.	
27. Solution should have an intelligent load-balancing of resources that allow parallel Replication of VMs to reduce replication windows	
28. Solution must have the ability to facilitate large scale recovery by creating sophisticated DR plans and automatically executing them (i.e. application-specific steps)	
29. Solution should be able to create rich DR documentation, run test plans and verify application consistency	
30. Solution should support multi-factor authentication (MFA) for additional user verification, combined with login and password credentials, to provide more secure access to the console and protect user accounts from being compromised	
31. Solution must support multi-tenancy	

Description	**Comply (Yes/No)**
Technical Terms and Conditions	
1. The bidder shall have at least two certified engineers according to the manufacturer's recommendations on the proposed solution; at least one of them shall be assigned to the project with EHS.	
2. The bidder must be an authorized Partner of the mother company he represents in this bid; the highest two partnership levels are only accepted. The bidder must submit an up-to-date valid official letter/certificate from the mother company as part of the bidder's qualification documents.	
3. The bidder shall have at least five enterprise scale live installations for similar solution. The references for such project must be provided within the proposal in order to be contacted by EHS as part of the technical evaluation.	

Description	Comply (Yes/No)
Warranty and Support	
1. The bidder shall offer minimum of (5) years (8/5) manufacturer warranty and support service. Vendor's support contract number / ID shall be provided to EHS.	
2. The bidder shall offer minimum of (5) years (24/7) local maintenance and support service; Maintenance and support service shall cover all supplied components and services.	
3. The Warranty and support services starting date is the date of the EHS's final acceptations of the completed scope of work.	
4. During the warranty period, the supplier shall provide all required spare parts free of charge.	
5. The warranty period covers support on site.	
6. The bidder shall provide the support approach in the form of a signed and stamped SLA, including the escalation matrix, support contacts, and response time.	
7. The bidder shall provide the yearly cost of the vendor's support service for additional one year, two years and five years after the five years of the product support end.	
8. Perform preventive maintenance for the delivered solution based on four yearly visits during the warranty and support period.	

Description	Comply (Yes/No)
License	
1. Provide the licenses of any/all features that require purchasing a specific license to enable and use. Further, describe how licenses are to be validated or enforced.	
2. All the licenses required for the solution must be perpetual licenses or for five years.	
3. The vendor shall provide how solution licensing is deployed.	
4. The supplier shall provide EHS the required licenses in the name of EHS to access and use the Software supplied through this RFP.	

Description	Comply (Yes/No)
End-of-Life and End-of-Sale Conditions	
1. The equipment quoted by the bidder should not be declared as End of Life (EOL) or End of Sale (EOS) by the manufacturer, at the time of bidding.	
2. The bidder must provide a 5-year lifetime letter of the solution from the vendor.	

Description	Comply (Yes/No)
Product origin	
1. The mother company shall be from the USA, Europe, or Japan.	
2. The Solution should be a Leader in Magic Quadrant for Enterprise Backup and Recovery Software Solutions	

35. Lot (2): Service Level Agreement - MOH

SLA Scope

The scope of this SLA agreement covers the provided solution for Backup and Data Protection Solution including all hardware and software components. On-site labor and parts must also be included.

SLA Duration

The supplier must provide maintenance and support for hardware and software for a period of five years starting the date of the EHS's final acceptations of the completed scope of work.

SLA Terms and conditions

The supplier response will be measured and monitored using EHS's Service Management tool.

During the Maintenance period, the supplier must provide the following:

- Preventive maintenance program and provide preventive maintenance scheduled visit every three months.
- Health check report after every preventive visit.
- Support methodology and escalation matrix including contacts details.
- Manufacturer support for all components.
- Maintaining spare parts to meet the "availability" target at no additional cost.
- Support, configure and resolve problems whenever needed and/or if requested by EHS.
- Commit to providing quality assurance for any major configuration changes whenever requested by EHS. Any change must be done within the EHS's Change Management process.
- Perform Firmware updates, patches, and new releases according to the manufacturer's recommendation
- Handle all support requests submitted within or outside working hours without extra charges.
- Provide the required assistance to EHS staff for any configuration modification.
- All the solution's components should be covered back-to-back by Vendor support without any exception; the supplier shall provide the approach to validate the support contract with the vendor to EHS.

Support Cases Management

EHS will set the support cases Severity level upon opening each individual support case.

Support cases covered by this agreement are to be treated by supplier according to the ITIL V4 framework incident management process and request fulfillment process, inline with the supplier provided support structure.

SLA Severity Levels and Targets

Severity Level 1: Critical

Definition:

This level represents incidents causing a critical impact to the business, resulting in severe disruption or complete unavailability of a critical system or service.

Examples:

- Complete system outage affecting all users.
- Security breach leading to unauthorized access to sensitive data.
- Data corruption or loss with significant business impact.

Response Time:

Immediate response required, typically within 1 hour.

Response Time Schedule:

24/7

Severity Level 2: High

Definition:

Incidents with high impact but not immediately critical, causing significant disruption or degradation in services.

Examples:

1. Major performance degradation affecting a critical business process.
2. Service interruptions affecting a specific department or location.
3. A security vulnerability that requires urgent attention.

Response Time:

Response within 2 hours.

Response Time Schedule:

24/7

Severity Level 3: Medium

Definition:

Incidents causing a moderate impact, resulting in disruption or degradation of non-critical services or affecting a limited number of users.

Examples:

- Performance issues affecting non-essential services.
- Application errors causing inconvenience but not critical to operations.
- Limited data loss with backups available for recovery.

Response Time:

Response within 4 hours.

Response Time Schedule:

Eight business-working hours - 5 Weekdays Excluding Holidays

Severity Level 4: Low

Definition:

Incidents causing minor impact, resulting in minimal disruption or inconvenience to users or business operations.

Examples:

- Minor performance issues with no critical impact.
- Non-urgent software or application bugs.
- Requests for information or non-urgent assistance.

Response Time:

Response within one business day.

Response Time Schedule:

Eight business-working hours - 5 Weekdays Excluding Holidays

During the resolution process of any problem, EHS team shall stay informed about the progress of the resolution process.

Following the completion of any service related to incident resolution (Severity Level 1 and Severity Level 2) and after closing the incident, the supplier shall provide an incident report. The Report shall include the Root Cause Analysis “RCA” and indicate the exact time at which an intervention began, the components that was serviced or replaced, the corrective measures that were taken, and the amount of time needed for the intervention since the manifestation of the problem until functionality is restored.

Response time: is the time it takes a provider to respond to an inquiry or request from a client.

SLA Availability Target and Penalties

Additional hours exceeding the allowable downtime will be subject to penalty. The minimum accepted system availability is 99.9% yearly uptime.

Throughout the execution of the SLA, vendors should not rely on system redundancy as a **permanent** resolution

The bidder will be subject to penalty if he does not meet the “response time”. The following table shows all the penalties under this SLA contract. In addition, the “response time” must be met with each Severity Level.

Penalty condition	Penalty amount per hour JoD			
	Severity Level 1	Severity Level 2	Severity Level 3	Severity Level 4
Failed to achieve 99.9% availability target	400	300	0	0
Failed to achieve "response time"	400	300	100	50

Availability: the ability of an IT system to perform its agreed function as required.

Electronic Health Solutions