



*Empowered lives.
Resilient nations.*

INVITATION TO BID

Procurement of Information Systems for Izmir Model Factory

ITB No.: UNDP-TUR-ITB(MC1)-2021/008

Project: Turkey Resilience Project in Response to the Syria Crisis, Component 1 – Job Creation

Country: Turkey

Issued on: 20 May 2021

Contents

Section 1. Letter of Invitation.....	4
Section 2. Instruction to Bidders.....	6
GENERAL PROVISIONS	6
1. Introduction	6
2. Fraud & Corruption, Gifts and Hospitality	6
3. Eligibility	6
4. Conflict of Interests	7
B. PREPARATION OF BIDS	7
5. General Considerations	7
6. Cost of Preparation of Bid	8
7. Language	8
8. Documents Comprising the Bid	8
9. Documents Establishing the Eligibility and Qualifications of the Bidder	8
10. Technical Bid Format and Content	8
11. Price Schedule	8
12. Bid Security	8
13. Currencies	9
14. Joint Venture, Consortium or Association	9
15. Only One Bid	10
16. Bid Validity Period	10
17. Extension of Bid Validity Period	10
18. Clarification of Bid (from the Bidders)	11
19. Amendment of Bids	11
20. Alternative Bids	11
21. Pre-Bid Conference	11
C. SUBMISSION AND OPENING OF BIDS.....	12
22. Submission	12
Hard copy (manual) submission	12
Email and eTendering submissions	12
23. Deadline for Submission of Bids and Late Bids	12
24. Withdrawal, Substitution, and Modification of Bids	13
25. Bid Opening	13
D. EVALUATION OF BIDS	13
26. Confidentiality	13
27. Evaluation of Bids	13
28. Preliminary Examination	14
29. Evaluation of Eligibility and Qualification	14
30. Evaluation of Technical Bid and prices	14
31. Due diligence	14
32. Clarification of Bids	15
33. Responsiveness of Bid	15
34. Nonconformities, Reparable Errors and Omissions	15
E. AWARD OF CONTRACT	16
35. Right to Accept, Reject, Any or All Bids	16
36. Award Criteria	16
37. Debriefing	16
38. Right to Vary Requirements at the Time of Award	16
39. Contract Signature	16
40. Contract Type and General Terms and Conditions	16
41. Performance Security	16
42. Bank Guarantee for Advanced Payment	16
43. Liquidated Damages	17
44. Payment Provisions	17
45. Vendor Protest	17
46. Other Provisions	17
Section 3. Bid Data Sheet.....	18
Section 4. Evaluation Criteria.....	24
Section 5a: Schedule of Requirements and Technical Specifications	26

Section 5b: Other Related Requirements.....93

Section 6: Returnable Bidding Forms / Checklist.....96

Form A: Bid Submission Form..... 97

Form B: Bidder Information Form..... 98

Form D: Eligibility and Qualification Form 100

Form E: Format of Technical Bid 102

FORM F: Price Schedule Form 194

FORM G: Form of Bid Security 196

Section 1. Letter of Invitation

The United Nations Development Programme (UNDP) hereby invites you to submit a Bid to this Invitation to Bid (ITB) for the above-referenced subject.

This ITB includes the following documents and the General Terms and Conditions of Contract which is inserted in the Bid Data Sheet:

- Section 1: This Letter of Invitation
- Section 2: Instruction to Bidders
- Section 3: Bid Data Sheet (BDS)
- Section 4: Evaluation Criteria
- Section 5: Schedule of Requirements and Technical Specifications
- Section 6: Returnable Bidding Forms
 - Form A: Bid Submission Form
 - Form B: Bidder Information Form
 - Form D: Qualification Form
 - Form E: Format of Technical Bid
 - Form F: Price Schedule
 - Form G: Form of Bid Security

Please be informed that this procurement process is being conducted through the online tendering system of UNDP. Bidders who wish to submit an offer must be registered in the system.

- Visit this page for system user guides and videos in different languages:

<http://www.undp.org/content/undp/en/home/operations/procurement/business/procurementnotices/resources/>

- If already registered, go to <https://etendering.partneragencies.org> and sign in using your username and password.
- Use “Forgotten password” link if you do not remember your password. Do not create a new profile.
- If you have never registered in the system before, you can register by visiting the link below and follow the instructions in the user guide (attached): <https://etendering.partneragencies.org>
 - Username: event.guest
 - Password: why2change
- It is strongly recommended to create a username with two parts: your first name and last name separated by a “.”, (similar to the one shown above). Once registered you will receive a valid password to the registered email address which you can use for signing in and changing your password.
- Please note that your new password should meet the following criteria:
 - Minimum 8 characters
 - At least one UPPERCASE LETTER

- At least one lowercase letter
- At least one number

You can view and download tender documents with the guest account as per the above username and password, However, if you are interested to participate, you must register in the system and subscribe to this tender to be notified when amendments are made.

E-Mail and Hard Copy Submissions are not accepted. Bids shall be submitted through e-tendering only.

If you are interested in submitting a Bid in response to this ITB, please prepare your Bid in accordance with the requirements and procedure as set out in this ITB and submit it by the “Deadline for Submission of Bids” set out in the eTendering System. Note that e-tendering system time zone is in **EST/EDT (New York)** time zone.

Please acknowledge receipt of this ITB by utilizing the “Accept Invitation” function in eTendering system. This will enable you to receive amendments or updates to the ITB. Should you require further clarifications, kindly communicate with the contact person identified in the attached Data Sheet as the focal point for queries on this ITB.

UNDP looks forward to receiving your Bid and thank you in advance for your interest in UNDP procurement opportunities.

Sincerely;

UNDP TURKEY Country Office

Section 2. Instruction to Bidders

GENERAL PROVISIONS

1. Introduction	1.1 Bidders shall adhere to all the requirements of this ITB, including any amendments made in writing by UNDP. This ITB is conducted in accordance with the UNDP Programme and Operations Policies and Procedures (POPP) on Contracts and Procurement which can be accessed at https://popp.undp.org/SitePages/POPPBSUnit.aspx?TermID=254a9f96-b883-476a-8ef8-e81f93a2b38d 1.2 Any Bid submitted will be regarded as an offer by the Bidder and does not constitute or imply the acceptance of the Bid by UNDP. UNDP is under no obligation to award a contract to any Bidder as a result of this ITB. 1.3 UNDP reserves the right to cancel the procurement process at any stage without any liability of any kind for UNDP, upon notice to the bidders or publication of cancellation notice on UNDP website. 1.4 As part of the bid, it is desired that the Bidder registers at the United Nations Global Marketplace (UNGM) website (www.ungm.org). The Bidder may still submit a bid even if not registered with the UNGM. However, if the Bidder is selected for contract award, the Bidder must register on the UNGM prior to contract signature.
2. Fraud & Corruption, Gifts and Hospitality	2.1 UNDP strictly enforces a policy of zero tolerance on proscribed practices, including fraud, corruption, collusion, unethical or unprofessional practices, and obstruction of UNDP vendors and requires all bidders/vendors observe the highest standard of ethics during the procurement process and contract implementation. UNDP's Anti-Fraud Policy can be found at http://www.undp.org/content/undp/en/home/operations/accountability/audit/office_of_audit_andinvestigation.html#anti 2.2 Bidders/vendors shall not offer gifts or hospitality of any kind to UNDP staff members including recreational trips to sporting or cultural events, theme parks or offers of holidays, transportation, or invitations to extravagant lunches or dinners. 2.3 In pursuance of this policy, UNDP: (a) Shall reject a bid if it determines that the selected bidder has engaged in any corrupt or fraudulent practices in competing for the contract in question; (b) Shall declare a vendor ineligible, either indefinitely or for a stated period, to be awarded a contract if at any time it determines that the vendor has engaged in any corrupt or fraudulent practices in competing for, or in executing a UNDP contract. 2.4 All Bidders must adhere to the UN Supplier Code of Conduct, which may be found at https://www.un.org/Depts/ptd/about-us/un-supplier-code-conduct
3. Eligibility	3.1 A vendor should not be suspended, debarred, or otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization. Vendors are therefore required to disclose to UNDP whether they are subject to any sanction or temporary suspension imposed by

	these organizations. 3.2 It is the Bidder's responsibility to ensure that its employees, joint venture members, sub-contractors, service providers, suppliers and/or their employees meet the eligibility requirements as established by UNDP.
4. Conflict of Interests	4.1 Bidders must strictly avoid conflicts with other assignments or their own interests, and act without consideration for future work. Bidders found to have a conflict of interest shall be disqualified. Without limitation on the generality of the above, Bidders, and any of their affiliates, shall be considered to have a conflict of interest with one or more parties in this solicitation process, if they: a) Are or have been associated in the past, with a firm or any of its affiliates which have been engaged by UNDP to provide services for the preparation of the design, specifications, Terms of Reference, cost analysis/estimation, and other documents to be used for the procurement of the goods and services in this selection process; b) Were involved in the preparation and/or design of the programme/project related to the goods and/or services requested under this ITB; or c) Are found to be in conflict for any other reason, as may be established by, or at the discretion of UNDP. 4.2 In the event of any uncertainty in the interpretation of a potential conflict of interest, Bidders must disclose to UNDP, and seek UNDP's confirmation on whether or not such conflict exists. 4.3 Similarly, the Bidders must disclose in their Bid their knowledge of the following: a) If the owners, part-owners, officers, directors, controlling shareholders, of the bidding entity or key personnel who are family members of UNDP staff involved in the procurement functions and/or the Government of the country or any Implementing Partner receiving goods and/or services under this ITB; and b) All other circumstances that could potentially lead to actual or perceived conflict of interest, collusion or unfair competition practices. Failure to disclose such an information may result in the rejection of the Bid or Bids affected by the non-disclosure. 4.4 The eligibility of Bidders that are wholly or partly owned by the Government shall be subject to UNDP's further evaluation and review of various factors such as being registered, operated and managed as an independent business entity, the extent of Government ownership/share, receipt of subsidies, mandate and access to information in relation to this ITB, among others. Conditions that may lead to undue advantage against other Bidders may result in the eventual rejection of the Bid.
B. PREPARATION OF BIDS	
5. General Considerations	5.1 In preparing the Bid, the Bidder is expected to examine the ITB in detail. Material deficiencies in providing the information requested in the ITB may result in rejection of the Bid. 5.2 The Bidder will not be permitted to take advantage of any errors or omissions in the ITB. Should such errors or omissions be discovered, the Bidder must

	notify the UNDP accordingly.
6. Cost of Preparation of Bid	6.1 The Bidder shall bear all costs related to the preparation and/or submission of the Bid, regardless of whether its Bid is selected or not. UNDP shall not be responsible or liable for those costs, regardless of the conduct or outcome of the procurement process.
7. Language	7.1 The Bid, as well as any and all related correspondence exchanged by the Bidder and UNDP, shall be written in the language (s) specified in the BDS.
8. Documents Comprising the Bid	8.1 The Bid shall comprise of the following documents and related forms which details are provided in the BDS: a) Documents Establishing the Eligibility and Qualifications of the Bidder; b) Technical Bid; c) Price Schedule; d) Bid Security, if required by BDS; e) Any attachments and/or appendices to the Bid.
9. Documents Establishing the Eligibility and Qualifications of the Bidder	9.1 The Bidder shall furnish documentary evidence of its status as an eligible and qualified vendor, using the Forms provided under Section 6 and providing documents required in those forms. In order to award a contract to a Bidder, its qualifications must be documented to UNDP's satisfaction.
10. Technical Bid Format and Content	10.1 The Bidder is required to submit a Technical Bid using the Standard Forms and templates provided in Section 6 of the ITB. 10.2 Samples of items, when required as per Section 5, shall be provided within the time specified and unless otherwise specified by the Purchaser, at no expense to the UNDP. If not destroyed by testing, samples will be returned at Bidder's request and expense, unless otherwise specified. 10.3 When applicable and required as per Section 5, the Bidder shall describe the necessary training programme available for the maintenance and operation of the equipment offered as well as the cost to the UNDP. Unless otherwise specified, such training as well as training materials shall be provided in the language of the Bid as specified in the BDS. 10.4 When applicable and required as per Section 5, the Bidder shall certify the availability of spare parts for a period of at least five (5) years from date of delivery, or as otherwise specified in this ITB.
11. Price Schedule	11.1 The Price Schedule shall be prepared using the Form provided in Section 6 of the ITB and taking into consideration the requirements in the ITB. 11.2 Any requirement described in the Technical Bid but not priced in the Price Schedule, shall be assumed to be included in the prices of other activities or items, as well as in the final total price.
12. Bid Security	12.1 A Bid Security, if required by BDS, shall be provided in the amount and form indicated in the BDS. The Bid Security shall be valid for a minimum of thirty (30) days after the final date of validity of the Bid. 12.2 The Bid Security shall be included along with the Bid. If Bid Security is required

	by the ITB but is not found in the Bid, the offer shall be rejected. 12.3 If the Bid Security amount or its validity period is found to be less than what is required by UNDP, UNDP shall reject the Bid. 12.4 In the event an electronic submission is allowed in the BDS, Bidders shall include a copy of the Bid Security in their bid and the original of the Bid Security must be sent via courier or hand delivery as per the instructions in BDS. 12.5 The Bid Security may be forfeited by UNDP, and the Bid rejected, in the event of any, or combination, of the following conditions: a) If the Bidder withdraws its offer during the period of the Bid Validity specified in the BDS, or; b) In the event the successful Bidder fails: i. to sign the Contract after UNDP has issued an award; or ii. to furnish the Performance Security, insurances, or other documents that UNDP may require as a condition precedent to the effectivity of the contract that may be awarded to the Bidder.
13. Currencies	13.1 All prices shall be quoted in the currency or currencies indicated in the BDS. Where Bids are quoted in different currencies, for the purposes of comparison of all Bids: a) UNDP will convert the currency quoted in the Bid into the UNDP preferred currency, in accordance with the prevailing UN operational rate of exchange on the last day of submission of Bids; and b) In the event that UNDP selects a Bid for award that is quoted in a currency different from the preferred currency in the BDS, UNDP shall reserve the right to award the contract in the currency of UNDP's preference, using the conversion method specified above.
14. Joint Venture, Consortium or Association	14.1 If the Bidder is a group of legal entities that will form or have formed a Joint Venture (JV), Consortium or Association for the Bid, they shall confirm in their Bid that : (i) they have designated one party to act as a lead entity, duly vested with authority to legally bind the members of the JV, Consortium or Association jointly and severally, which shall be evidenced by a duly notarized Agreement among the legal entities, and submitted with the Bid; and (ii) if they are awarded the contract, the contract shall be entered into, by and between UNDP and the designated lead entity, who shall be acting for and on behalf of all the member entities comprising the joint venture. 14.2 After the Deadline for Submission of Bid, the lead entity identified to represent the JV, Consortium or Association shall not be altered without the prior written consent of UNDP. 14.3 The lead entity and the member entities of the JV, Consortium or Association shall abide by the provisions of Clause 9 herein in respect of submitting only one Bid. 14.4 The description of the organization of the JV, Consortium or Association must clearly define the expected role of each of the entities in the joint venture in delivering the requirements of the ITB, both in the Bid and the JV, Consortium or Association Agreement. All entities that comprise the JV, Consortium or Association shall be subject to the eligibility and qualification assessment by

	UNDP. 14.5 A JV, Consortium or Association in presenting its track record and experience should clearly differentiate between: a) Those that were undertaken together by the JV, Consortium or Association; and b) Those that were undertaken by the individual entities of the JV, Consortium or Association. 14.6 Previous contracts completed by individual experts working privately but who are permanently or were temporarily associated with any of the member firms cannot be claimed as the experience of the JV, Consortium or Association or those of its members, but should only be claimed by the individual experts themselves in their presentation of their individual credentials 14.7 JV, Consortium or Associations are encouraged for high value, multi-sectoral requirements when the spectrum of expertise and resources required may not be available within one firm.
15. Only One Bid	15.1 The Bidder (including the individual members of any Joint Venture) shall submit only one Bid, either in its own name or as part of a Joint Venture. 15.2 Bids submitted by two (2) or more Bidders shall all be rejected if they are found to have any of the following: a) they have at least one controlling partner, director or shareholder in common; or b) any one of them receive or have received any direct or indirect subsidy from the other/s; or c) they have the same legal representative for purposes of this ITB; or d) they have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about, or influence on the Bid of another Bidder regarding this ITB process; e) they are subcontractors to each other's Bid, or a subcontractor to one Bid also submits another Bid under its name as lead Bidder; or some key personnel proposed to be in the team of one Bidder participates in more than one Bid received for this ITB process. This condition relating to the personnel, does not apply to subcontractors being included in more than one Bid.
16. Bid Validity Period	16.1 Bids shall remain valid for the period specified in the BDS, commencing on the Deadline for Submission of Bids. A Bid valid for a shorter period may be rejected by UNDP and rendered non-responsive. 16.2 During the Bid validity period, the Bidder shall maintain its original Bid without any change, including the availability of the Key Personnel, the proposed rates and the total price.
17. Extension of Bid Validity Period	17.1 In exceptional circumstances, prior to the expiration of the Bid validity period, UNDP may request Bidders to extend the period of validity of their Bids. The request and the responses shall be made in writing, and shall be considered integral to the Bid. 17.2 If the Bidder agrees to extend the validity of its Bid, it shall be done without any change to the original Bid.

	17.3 The Bidder has the right to refuse to extend the validity of its Bid, in which case, the Bid shall not be further evaluated.
18. Clarification of Bid (from the Bidders)	18.1 Bidders may request clarifications on any of the ITB documents no later than the date indicated in the BDS. Any request for clarification must be sent in writing in the manner indicated in the BDS. If inquiries are sent other than specified channel, even if they are sent to a UNDP staff member, UNDP shall have no obligation to respond or confirm that the query was officially received. 18.2 UNDP will provide the responses to clarifications through the method specified in the BDS. 18.3 UNDP shall endeavour to provide responses to clarifications in an expeditious manner, but any delay in such response shall not cause an obligation on the part of UNDP to extend the submission date of the Bids, unless UNDP deems that such an extension is justified and necessary.
19. Amendment of Bids	19.1 At any time prior to the deadline of Bid submission, UNDP may for any reason, such as in response to a clarification requested by a Bidder, modify the ITB in the form of an amendment to the ITB. Amendments will be made available to all prospective bidders. 19.2 If the amendment is substantial, UNDP may extend the Deadline for submission of Bid to give the Bidders reasonable time to incorporate the amendment into their Bids.
20. Alternative Bids	20.1 Unless otherwise specified in the BDS, alternative Bids shall not be considered. If submission of alternative Bid is allowed by BDS, a Bidder may submit an alternative Bid, but only if it also submits a Bid conforming to the ITB requirements. Where the conditions for its acceptance are met, or justifications are clearly established, UNDP reserves the right to award a contract based on an alternative Bid. 20.2 If multiple/alternative bids are being submitted, they must be clearly marked as "Main Bid" and "Alternative Bid"
21. Pre-Bid Conference	21.1 When appropriate, a pre-bid conference will be conducted at the date, time and location specified in the BDS. All Bidders are encouraged to attend. Non-attendance, however, shall not result in disqualification of an interested Bidder. Minutes of the Bidder's conference will be disseminated on the procurement website and shared by email or on the e-Tendering platform as specified in the BDS. No verbal statement made during the conference shall modify the terms and conditions of the ITB, unless specifically incorporated in the Minutes of the Bidder's Conference or issued/posted as an amendment to ITB.

c. SUBMISSION AND OPENING OF BIDS

22. Submission	22.1 The Bidder shall submit a duly signed and complete Bid comprising the documents and forms in accordance with requirements in the BDS. The Price Schedule shall be submitted together with the Technical Bid. Bid can be delivered either personally, by courier, or by electronic method of transmission as specified in the BDS. 22.2 The Bid shall be signed by the Bidder or person(s) duly authorized to commit the Bidder. The authorization shall be communicated through a document evidencing such authorization issued by the legal representative of the bidding entity, or a Power of Attorney, accompanying the Bid. 22.3 Bidders must be aware that the mere act of submission of a Bid, in and of itself, implies that the Bidder fully accepts the UNDP General Contract Terms and Conditions.
Hard copy (manual) submission	22.4 Hard copy (manual) submission by courier or hand delivery allowed or specified in the BDS shall be governed as follows: a) The signed Bid shall be marked "Original", and its copies marked "Copy" as appropriate. The number of copies is indicated in the BDS. All copies shall be made from the signed original only. If there are discrepancies between the original and the copies, the original shall prevail. (b) The Technical Bid and Price Schedule must be sealed and submitted together in an envelope, which shall: - Bear the name of the Bidder; - Be addressed to UNDP as specified in the BDS; and - Bear a warning not to open before the time and date for Bid opening as specified in the BDS. If the envelope with the Bid is not sealed and marked as required, UNDP shall assume no responsibility for the misplacement, loss, or premature opening of the Bid.
Email and eTendering submissions	22.5 Electronic submission through email or eTendering, if allowed as specified in the BDS, shall be governed as follows: - Electronic files that form part of the Bid must be in accordance with the format and requirements indicated in BDS; - Documents which are required to be in original form (e.g. Bid Security, etc.) must be sent via courier or hand delivered as per the instructions in BDS. 22.6 Detailed instructions on how to submit, modify or cancel a bid in the eTendering system are provided in the eTendering system Bidder User Guide and Instructional videos available on this link: http://www.undp.org/content/undp/en/home/operations/procurement/business/procurement-notice/resources/
23. Deadline for Submission of Bids and Late Bids	23.1 Complete Bids must be received by UNDP in the manner, and no later than the date and time, specified in the BDS. UNDP shall only recognise the actual date and time that the bid was received by UNDP 23.2 UNDP shall not consider any Bid that is received after the deadline for the

	submission of Bids.
24. Withdrawal, Substitution, and Modification of Bids	24.1 A Bidder may withdraw, substitute or modify its Bid after it has been submitted at any time prior to the deadline for submission. 24.2 Manual and Email submissions: A bidder may withdraw, substitute or modify its Bid by sending a written notice to UNDP, duly signed by an authorized representative, and shall include a copy of the authorization (or a Power of Attorney). The corresponding substitution or modification of the Bid, if any, must accompany the respective written notice. All notices must be submitted in the same manner as specified for submission of Bids, by clearly marking them as "WITHDRAWAL" "SUBSTITUTION," or "MODIFICATION" 24.3 eTendering: A Bidder may withdraw, substitute or modify its Bid by Cancelling, Editing, and re-submitting the Bid directly in the system. It is the responsibility of the Bidder to properly follow the system instructions, duly edit and submit a substitution or modification of the Bid as needed. Detailed instructions on how to cancel or modify a Bid directly in the system are provided in the Bidder User Guide and Instructional videos. 24.4 Bids requested to be withdrawn shall be returned unopened to the Bidders (only for manual submissions), except if the bid is withdrawn after the bid has been opened.
25. Bid Opening	25.1 UNDP will open the Bid in the presence of an ad-hoc committee formed by UNDP of at least two (2) members. 25.2 The Bidders' names, modifications, withdrawals, the condition of the envelope labels/seals, the number of folders/files and all other such other details as UNDP may consider appropriate, will be announced at the opening. No Bid shall be rejected at the opening stage, except for late submissions, in which case, the Bid shall be returned unopened to the Bidders. 25.3 In the case of e-Tendering submission, bidders will receive an automatic notification once the Bid is opened.
D. EVALUATION OF BIDS	
26. Confidentiality	26.1 Information relating to the examination, evaluation, and comparison of Bids, and the recommendation of contract award, shall not be disclosed to Bidders or any other persons not officially concerned with such process, even after publication of the contract award. 26.2 Any effort by a Bidder or anyone on behalf of the Bidder to influence UNDP in the examination, evaluation and comparison of the Bids or contract award decisions may, at UNDP's decision, result in the rejection of its Bid and may subsequently be subject to the application of prevailing UNDP's vendor sanctions procedures.
27. Evaluation of Bids	27.1 UNDP will conduct the evaluation solely on the basis of the Bids received. 27.2 Evaluation of Bids shall be undertaken in the following steps: a) Preliminary Examination including Eligibility b) Arithmetical check and ranking of bidders who passed preliminary examination by price. c) Qualification assessment (if pre-qualification was not done)

	a) Evaluation of Technical Bids b) Evaluation of prices Detailed evaluation will be focussed on the 3 - 5 lowest priced bids. Further higher priced bids shall be added for evaluation if necessary
28. Preliminary Examination	28.1 UNDP shall examine the Bids to determine whether they are complete with respect to minimum documentary requirements, whether the documents have been properly signed, and whether the Bids are generally in order, among other indicators that may be used at this stage. UNDP reserves the right to reject any Bid at this stage.
29. Evaluation of Eligibility and Qualification	29.1 Eligibility and Qualification of the Bidder will be evaluated against the Minimum Eligibility/Qualification requirements specified in the Section 4 (Evaluation Criteria). 29.2 In general terms, vendors that meet the following criteria may be considered qualified: a) They are not included in the UN Security Council 1267/1989 Committee's list of terrorists and terrorist financiers, and in UNDP's ineligible vendors' list; b) They have a good financial standing and have access to adequate financial resources to perform the contract and all existing commercial commitments, c) They have the necessary similar experience, technical expertise, production capacity, quality certifications, quality assurance procedures and other resources applicable to the supply of goods and/or services required; d) They are able to comply fully with the UNDP General Terms and Conditions of Contract; e) They do not have a consistent history of court/arbitral award decisions against the Bidder; and f) They have a record of timely and satisfactory performance with their clients.
30. Evaluation of Technical Bid and prices	30.1 The evaluation team shall review and evaluate the Technical Bids on the basis of their responsiveness to the Schedule of Requirements and Technical Specifications and other documentation provided, applying the procedure indicated in the BDS and other ITB documents. When necessary, and if stated in the BDS, UNDP may invite technically responsive bidders for a presentation related to their technical Bids. The conditions for the presentation shall be provided in the bid document where required.
31. Due diligence	31.1 UNDP reserves the right to undertake a due diligence exercise, aimed at determining to its satisfaction, the validity of the information provided by the Bidder. Such exercise shall be fully documented and may include, but need not be limited to, all or any combination of the following: a) Verification of accuracy, correctness and authenticity of information provided by the Bidder; b) Validation of extent of compliance to the ITB requirements and evaluation criteria based on what has so far been found by the evaluation team; c) Inquiry and reference checking with Government entities with jurisdiction on the Bidder, or with previous clients, or any other entity that may have done business with the Bidder;

	d) Inquiry and reference checking with previous clients on the performance on on-going or completed contracts, including physical inspections of previous works, as deemed necessary; e) Physical inspection of the Bidder's offices, branches or other places where business transpires, with or without notice to the Bidder; f) Other means that UNDP may deem appropriate, at any stage within the selection process, prior to awarding the contract.
32. Clarification of Bids	32.1 To assist in the examination, evaluation and comparison of Bids, UNDP may, at its discretion, request any Bidder for a clarification of its Bid. 32.2 UNDP's request for clarification and the response shall be in writing and no change in the prices or substance of the Bid shall be sought, offered, or permitted, except to provide clarification, and confirm the correction of any arithmetic errors discovered by UNDP in the evaluation of the Bids, in accordance with the ITB. 32.3 Any unsolicited clarification submitted by a Bidder in respect to its Bid, which is not a response to a request by UNDP, shall not be considered during the review and evaluation of the Bids.
33. Responsiveness of Bid	33.1 UNDP's determination of a Bid's responsiveness will be based on the contents of the bid itself. A substantially responsive Bid is one that conforms to all the terms, conditions, specifications and other requirements of the ITB without material deviation, reservation, or omission. 33.2 If a bid is not substantially responsive, it shall be rejected by UNDP and may not subsequently be made responsive by the Bidder by correction of the material deviation, reservation, or omission.
34. Nonconformities, Repairable Errors and Omissions	34.1 Provided that a Bid is substantially responsive, UNDP may waive any non-conformities or omissions in the Bid that, in the opinion of UNDP, do not constitute a material deviation. 34.2 UNDP may request the Bidder to submit the necessary information or documentation, within a reasonable period, to rectify nonmaterial nonconformities or omissions in the Bid related to documentation requirements. Such omission shall not be related to any aspect of the price of the Bid. Failure of the Bidder to comply with the request may result in the rejection of its Bid. 34.3 For the bids that have passed the preliminary examination, UNDP shall check and correct arithmetical errors as follows: a) if there is a discrepancy between the unit price and the line item total that is obtained by multiplying the unit price by the quantity, the unit price shall prevail and the line item total shall be corrected, unless in the opinion of UNDP there is an obvious misplacement of the decimal point in the unit price; in which case, the line item total as quoted shall govern and the unit price shall be corrected; b) if there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected; and c) if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an

	arithmetic error, in which case the amount in figures shall prevail. 34.4 If the Bidder does not accept the correction of errors made by UNDP, its Bid shall be rejected.
E. AWARD OF CONTRACT	
35. Right to Accept, Reject, Any or All Bids	35.1 UNDP reserves the right to accept or reject any bid, to render any or all of the bids as non-responsive, and to reject all Bids at any time prior to award of contract, without incurring any liability, or obligation to inform the affected Bidder(s) of the grounds for UNDP's action. UNDP shall not be obliged to award the contract to the lowest priced offer.
36. Award Criteria	36.1 Prior to expiration of the period of Bid validity, UNDP shall award the contract to the qualified and eligible Bidder that is found to be responsive to the requirements of the Schedule of Requirements and Technical Specification, and has offered the lowest price.
37. Debriefing	37.1 In the event that a Bidder is unsuccessful, the Bidder may request for a debriefing from UNDP. The purpose of the debriefing is to discuss the strengths and weaknesses of the Bidder's submission, in order to assist the Bidder in improving its future Bids for UNDP procurement opportunities. The content of other Bids and how they compare to the Bidder's submission shall not be discussed.
38. Right to Vary Requirements at the Time of Award	38.1 At the time of award of Contract, UNDP reserves the right to vary the quantity of goods and/or services, by up to a maximum twenty-five per cent (25%) of the total offer, without any change in the unit price or other terms and conditions.
39. Contract Signature	39.1 Within fifteen (15) days from the date of receipt of the Contract, the successful Bidder shall sign and date the Contract and return it to UNDP. Failure to do so may constitute sufficient grounds for the annulment of the award, and forfeiture of the Bid Security, if any, and on which event, UNDP may award the Contract to the Second highest rated or call for new Bids.
40. Contract Type and General Terms and Conditions	40.1 The types of Contract to be signed and the applicable UNDP Contract General Terms and Conditions, as specified in BDS, can be accessed at http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html
41. Performance Security	41.1 A performance security, if required in the BDS, shall be provided in the amount specified in BDS and form available at https://popp.undp.org/layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/PSU_Solicitation_Performance%20Guarantee%20Form.docx&action=default within a maximum of fifteen (15) days of the contract signature by both parties. Where a performance security is required, the receipt of the performance security by UNDP shall be a condition for rendering the contract effective.
42. Bank Guarantee for Advanced Payment	42.1 Except when the interests of UNDP so require, it is UNDP's standard practice to not make advance payment(s) (i.e., payments without having received any

	outputs). If an advance payment is allowed as per the BDS, and exceeds 20% of the total contract price, or USD 30,000, whichever is less, the Bidder shall submit a Bank Guarantee in the full amount of the advance payment in the form available at https://popp.undp.org/layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/PSU_Contract%20Management%20Payment%20and%20Taxes_Advanced%20Payment%20Guarantee%20Form.docx&action=default
43. Liquidated Damages	43.1 If specified in the BDS, UNDP shall apply Liquidated Damages for the damages and/or risks caused to UNDP resulting from the Contractor's delays or breach of its obligations as per Contract.
44. Payment Provisions	44.1 Payment will be made only upon UNDP's acceptance of the goods and/or services performed. The terms of payment shall be within thirty (30) days, after receipt of invoice and certification of acceptance of goods and/or services issued by the proper authority in UNDP with direct supervision of the Contractor. Payment will be effected by bank transfer in the currency of the contract.
45. Vendor Protest	45.1 UNDP's vendor protest procedure provides an opportunity for appeal to those persons or firms not awarded a contract through a competitive procurement process. In the event that a Bidder believes that it was not treated fairly, the following link provides further details regarding UNDP vendor protest procedures: http://www.undp.org/content/undp/en/home/procurement/business/protest-and-sanctions.html
46. Other Provisions	46.1 In the event that the Bidder offers a lower price to the host Government (e.g. General Services Administration (GSA) of the federal government of the United States of America) for similar goods and/or services, UNDP shall be entitled to the same lower price. The UNDP General Terms and Conditions shall have precedence. 46.2 UNDP is entitled to receive the same pricing offered by the same Contractor in contracts with the United Nations and/or its Agencies. The UNDP General Terms and Conditions shall have precedence. 46.3 The United Nations has established restrictions on employment of (former) UN staff who have been involved in the procurement process as per bulletin ST/SGB/2006/15 http://www.un.org/en/ga/search/view_doc.asp?symbol=ST/SGB/2006/15&referer

Section 3. Bid Data Sheet

The following data for the goods and/or services to be procured shall complement, supplement, or amend the provisions in the Invitation to Bid In the case of a conflict between the Instructions to Bidders, the Bid Data Sheet, and other annexes or references attached to the Bid Data Sheet, the provisions in the Bid Data Sheet shall prevail.

BDS No.	Ref. to Section.2	Data	Specific Instructions / Requirements
1	7	Language of the Bid	English
2		Submitting Bids for Parts or sub-parts of the Schedule of Requirements (partial bids)	Not Allowed
3	20	Alternative Bids	Shall not be considered
4	21	Pre-Bid conference	Will not be conducted
5	16	Bid Validity Period	90 days following bid submission deadline
6	13	Bid Security	Required in the amount of USD 5,000.00 Acceptable Forms of Bid Security: Bank Guarantee (See Section 6, Form G for the template) ▪ Bid Security shall be in English as per the template ▪ Currency of the Bid Security shall be in USD as per the amount indicated above ▪ No change shall be made to the template except for fields indicated in the template ▪ Bid Security shall be valid until 30 days after the expiry of Bid Validity Period. (i.e. 120 days after bid submission deadline) ▪ Original Bid Security shall be delivered to the below address on or before the submission deadline indicated in e-tendering system, with a PDF copy submitted as part of the electronic submission. Focal Point: Tunç Gürdal, Procurement Officer Yıldız Kule, 21st Floor, Dikmen Mahallesi, Turan Güneş Bulvarı, No:106, 06550, Çankaya, Ankara, Turkey

7	41	Advanced Payment upon signing of contract	Not Allowed
8	42	Liquidated Damages	Will be imposed as follows: Percentage of contract price per week (7 calendar days) of delay beyond 90 days after contract signature by UNDP and the contractor: 2% Max. number of weeks (7 calendar days) of delay is 5, after which UNDP reserves the right to terminate the contract.
9	40	Performance Security	Required in the amount of 10% of the total contract amount. Note: Performance Security will be a condition for signing of the contract. Contract will be signed after receipt of Performance Security from the successful bidder.
10	12	Currency of Bid	United States Dollar (USD)
11	31	Deadline for submitting requests for clarifications/ questions	7 days before the bid submission deadline
12	31	Contact Details for submitting clarifications/questions	Focal Person in UNDP: Tunç Gürdal, Procurement Officer Address: Yıldız Kule, Yukari Dikmen Mah. Turan Gunes Blv. No:106, 06550, Cankaya/Ankara/TURKEY E-mail address: : tr.procurement@undp.org
13	18, 19 and 21	Manner of Disseminating Supplemental Information to the ITB and responses/clarifications to queries	Posted directly to eTendering
14	22	Deadline for Submission	June 07, 2021, 07:00 am (EST/EDT New York Time) as indicated in the e-tendering System. Please note that system time zone is New York.
14	22	Allowable Manner of Submitting Bids	E-Tendering only EVENT ID: ITB-21-008 This procurement process is being conducted through the online tendering system of UNDP. Bidders who wish to submit an offer must be registered in the system. Visit this page for system user guides and videos in different languages: http://www.undp.org/content/undp/en/home/operations/procur

			ement/business/procurement-notices/resources/ If already registered, go to https://etendering.partneragencies.org and sign in using your username and password. Use "Forgotten password" link if you do not remember your password. Do not create a new profile. If you have never registered in the system before, you can register by visiting the link below and follow the instructions in the user guide (attached): https://etendering.partneragencies.org •Username: event.guest •Password: why2change It is strongly recommended to create a username with two parts: your first name and last name separated by a ".", (similar to the one shown above). Once registered you will receive a valid password to the registered email address which you can use for signing in and changing your password. Please note that your new password should meet the following criteria: • Minimum 8 characters • At least one UPPERCASE LETTER • At least one lowercase letter • At least one number You can view and download tender documents with the guest account as per the above username and password, However, if you are interested to participate, you must register in the system
15	22	Bid Submission Address	Bids shall be submitted through UNDP e-tendering system. Although bids shall be submitted through e-tendering, UNDP reserves the right to request original copies of the documents submitted as part of the bids during evaluation period, if required. Focal Point: Tunç Gürdal, Procurement Officer Yıldız Kule, 21st Floor, Dikmen Mahallesi, Turan Güneş Bulvarı, No:106, 06550, Çankaya, Ankara, Turkey

16	22	Electronic submission (email or eTendering) requirements	▪ Format: PDF files only ▪ File names must be maximum 60 characters long and must not contain any letter or special/Turkish character other than from Latin alphabet/keyboard. ▪ All files must be free of viruses and not corrupted. ▪ Max. File Size per transmission: 45 MB
17	25	Date, time and venue for the opening of bid	Bidders will receive notification through e-tendering when bids are opened.
18	27, 36	Evaluation Method for the Award of Contract	Lowest priced technically responsive, eligible and qualified bid.
19		Expected date for commencement of Contract	Contract is expected to be signed in July 2021
20		Maximum expected duration of contract	Delivery, installation and commissioning of all items shall be completed within 90 days after signature of the contract
21	35	UNDP will award the contract to:	One Bidder Only
22	39	Type of Contract	Contract for Goods and/or Services to UNDP http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html
23	39	UNDP Contract Terms and Conditions that will apply	UNDP General Terms and Conditions for Contracts http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html
24	44	Payment Provisions	1. 100% of contract price shall be paid within 30 days upon UNDP's issuance of Positive Inspection and Acceptance Report that indicates full compliance of the goods to Technical Specifications in this ITB and proper functioning of the whole system and receipt of invoice. Inspection and acceptance shall be conducted by a committee to be established by UNDP and the beneficiary/end user, following delivery, installation and commissioning of the whole system by the Contractor. 2. If a company established and operating in Turkey gets awarded by the contract, payment shall be made in Turkish Liras through conversion of the USD amount by the official UN Exchange Rate valid on the date of money transfer. Please refer to https://treasury.un.org/operationalrates/OperationalRates.php for UN Official Exchange Rate.

			3. In case a company established and operating in a country other than Turkey gets awarded by the contract, payment shall be effected in USD.
25		Taxation	<i>UN and its subsidiary organs are exempt from all taxes. Therefore, Bidders shall prepare their financial bids excluding Value Added Tax (VAT). It is the Bidder's responsibility to learn from relevant authorities (Ministry of Treasury and Finance) and/or to review /confirm published procedures and to consult with a certified financial consultant as needed to confirm the scope and procedures of VAT exemption application as per VAT Law, Ministry of Treasury and Finance General Communiqués. The contractor selected for the award shall not be entitled to receive any amount over its bid price in relation to VAT, Special Consumption Tax and any other applicable taxes. Overall contract amount to be paid to the contractor shall not exceed the total amount offered in the Financial Proposal.</i>
26	14	Joint Venture, Consortium or Association	Not allowed
27		Site Visit	Prospective bidders are encouraged to visit the site, at their own cost, at any time before submitting their bids, to ensure that they factor all parameters that would affect their bid as well as possible relevant costs. For bidders who would like to visit the site at their own expense, the bidders shall contact the UNDP Projects Coordinator, Ms. Ezgi Arslan via email address ezgi.arslan@undp.org for arrangement of the site visit. It is the bidders' responsibility to consider Covid-19 related risks in the case they visit the locations of the sites mentioned above. UNDP is not responsible for any Covid-19 related events and health issues that may arise during and after the site visits. UNDP shall not be responsible for the Bidders' inability to perform a site visit in any case and hence the successful bidder shall not be entitled to any payment during contract performance due to their failure to perform a site visit prior to submission of bids.
28		Other Information	1. Women owned and managed businesses are especially encouraged to apply to this ITB. 2. The documents that will be attached to Form B: Bidder Information Form (such as Certificate of Incorporation/Business Registration and Power of Attorney) can be submitted in local languages in the case that they are provided only in the local language by issuing authorities. In that case, the English translations of these documents shall be submitted by Proposers along with original documents in the local language. UNDP reserves the right to request notarized versions of these translations any time during the evaluation.

29		COVID-19 Specific Measures	The Bidders shall review all local regulations, as well as that of UN and UNDP concerning the measures they must take during performance of the contract in the context of COVID-19, before they submit their bids and factor relevant costs, if any, to their bids. The Contractor shall take all measures against COVID-19, imposed by local regulations as well as by UN and UNDP during performance of the contract, to protect health and social rights of its own personnel, as well as UNDP personnel, Project Stakeholders and third parties. Pursuant to "Clause 12- Indemnification" of UNDP General Terms and Conditions for Contracts (given in Item 40. "Contract Type and General Terms and Conditions" in Section 2. Instruction to Bidders of the ITB document) , the Contractor shall indemnify, defend, and hold and save harmless, UNDP, and its officials, agents and employees, from and against all suits, proceedings, claims, demands, losses and liability of any kind or nature brought by any third party against UNDP, including, but not limited to, all litigation costs and expenses, attorney's fees, settlement payments and damages, based on, arising from, or relating to COVID-19 measures that must be taken by the Contractor in the context of the contract. UNDP shall not be held accountable for any COVID-19 related health risks or events that are caused by negligence of the Contractor and/or any other third party.
----	--	----------------------------	---

Section 4. Evaluation Criteria

Preliminary Examination Criteria

Bids will be examined to determine whether they are complete and submitted in accordance with ITB requirements as per below criteria on a Yes/No basis:

- Appropriate signatures
- Power of Attorney
- Minimum Bid documents provided
- Bid Validity
- Bid Security submitted as per ITB requirements with compliant validity period

Minimum Eligibility and Qualification Criteria

Eligibility and Qualification will be evaluated on a Pass/Fail basis. (i.e. Any bidder who does not satisfy any one of these criteria shall be automatically eliminated from this procurement process.)

Subject	Criteria	Document Submission requirement
ELIGIBILITY		
Legal Status	▪ Vendor is a legally registered entity since May 2018. ▪ Vendor shall document that it has an established and registered office in Turkey	Form B: Bidder Information Form
Eligibility	Vendor is not suspended, nor debarred, nor otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization in accordance with ITB clause 3.	Form A: Bid Submission Form
Conflict of Interest	No conflicts of interest in accordance with ITB clause 4.	Form A: Bid Submission Form
Bankruptcy	Has not declared bankruptcy, is not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against the vendor that could impair its operations in the foreseeable future.	Form A: Bid Submission Form
Certificates and Licenses	▪ Duly authorized to act as Agent on behalf of the Manufacturer, or Power of Attorney, if bidder is not a manufacturer. Certificate of authorization shall be submitted along with the bid. ▪ Official appointment as local representative, if Bidder is submitting a Bid on behalf of an entity located outside the country. ▪ Certificate of Incorporation/ Business Registration ▪ Trade name registration papers, if applicable ▪ Signature Circular/Power of Attorney demonstrating authorization of the individual signing the Bid documents. ▪ Export/Import Licenses, if applicable.	Form B: Bidder Information Form

QUALIFICATION		
History of Non-Performing Contracts¹	Non-performance of a contract did not occur as a result of contractor default for the last 3 years.	Form D: Qualification Form
Litigation History	No consistent history of court/arbitral award decisions against the Bidder for the last 3 years.	Form D: Qualification Form
Previous Experience	Minimum 3 years of relevant experience.	Form D: Qualification Form
	Minimum one contract of similar value and nature completed as a prime contractor over the last 3 years*. Experiences that will be accepted as similar nature: Supply of IT Equipment *The reference period which will be taken into account will be the last 3 years from submission deadline. The start and end/completion dates of the references should be specified as day/month/year. Bidders shall submit Statements of Satisfactory Performance (i.e. Reference Letters, Work Completion Certificates) along with their bids.	Form D: Qualification Form
Financial Standing	Minimum average annual turnover of USD 250,000.00 for the last 3 years (i.e. 2018, 2019, 2020)*. *Bidders whose accounts have not yet been audited for 2020, shall submit audited financial statements for 2017, 2018, and 2019.	Form D: Qualification Form
	Bidder must demonstrate the current soundness of its financial standing and indicate its prospective long-term profitability by submitting their audited Financial Statements (balance sheets, including all related notes, and income statements).	Form D: Qualification Form
Technical Evaluation	The technical bids shall be evaluated on a pass/fail basis for compliance or non-compliance with the technical specifications identified in the bid document.	Form E: Technical Bid Form
Financial Evaluation	Detailed analysis of the price schedule based on requirements listed in Section 5 and quoted for by the bidders in Form F. Price comparison shall be based on the total turnkey price, including delivery. Comparison with budget/internal estimates.	Form F: Price Schedule Form
Other Information	Product catalogue/brochure of the proposed brand/model showing detailed technical specifications of the goods.	Form E: Technical Bid Form

¹ Non-performance, as decided by UNDP, shall include all contracts where (a) non-performance was not challenged by the contractor, including through referral to the dispute resolution mechanism under the respective contract, and (b) contracts that were so challenged but fully settled against the contractor. Non-performance shall not include contracts where Employers decision was overruled by the dispute resolution mechanism. Non-performance must be based on all information on fully settled disputes or litigation, i.e. dispute or litigation that has been resolved in accordance with the dispute resolution mechanism under the respective contract and where all appeal instances available to the Bidder have been exhausted.

Section 5a: Schedule of Requirements and Technical Specifications

Please be informed that that Turkish version of the specifications is given for reference purpose only. In case of an inconsistency between Turkish and English versions, English version shall prevail.

The number of the items to be delivered classified by item type is as follows:

Alınacak her bir malzeme türü için teslim edilecek sayılar aşağıdadır:

Item Type	Malzeme Türü	# of Items (Miktar)
Server	Sunucu	2
Data Storage Unit	Veri Depolama Ünitesi	1
Virtualization Software	Sanallaştırma Yazılımı	1
Backup Software	Yedekleme Yazılımı	1
Server Software	Sunucu Yazılımları	80 core Windows Server 2019 Standard licenses or equivalent 20 Windows Server 2019 Cal licenses or equivalent 2 SQL Server 2019 licenses or equivalent 20 SQL Server 2019 Cal licenses or equivalent
Backup Unit	Yedekleme Ünitesi	1
Network Switch Type 1	Ağ anahtarı Tip 1	1
Network Switch Type 2 (non-POE)	Ağ anahtarı Tip 2 (POE Olmayan)	2
Wireless Access Point	Kablosuz Erişim Noktası	7
Authentication and Network Access Control Software	Kimlik Doğrulama ve Ağ Erişim Kontrol Yazılımı	1
Firewall	Güvenlik Duvarı	1
Personal Computer	Bilgisayar	2
Data Center Security Software	Veri Merkezi Güvenlik Yazılımı	1
User Security Solution	Kullanıcı Güvenliği Çözümü	1
Uninterruptable Power Supply	Kesintisiz Güç Kaynağı	2

General requirements applying to all of the items:

- Updates for the proposed products must be available free of charge on the manufacturer's website.
- Documents and assembly apparatus related to all products such as CDs, brochures, manuals, etc. must be supplied with the products.
- The proposed products (including their parts) must not have been used before and must be sent in their original packaging without defects and damages, with all precautions taken against all kinds of impacts and damages.
- In a visible part of the device, the manufacturer will have a label indicating the company name, type, model, serial number, technical values, etc.
- Any announcement of End Of Life (EOL)/End Of Sale(EOS) must not have been done for any product to be offered.
- The product to be offered must be supported by the manufacturer for at least 5 years after the End Of Life (EOL) announcement is done.
- All units to be offered with the devices (GBIC, SFP, SFP+, QSFP, Direct Attach Cable, etc.) will have the same brand as the device and will not be OEM products.
- For each proposed product, the document

Tüm ürünler için geçerli genel şartlar:

- *Teklif edilen ürünlerin güncellemeleri üreticinin web sitesinden ücretsiz olarak temin edilebilmelidir.*
- *Tüm ürünler ile ilgili CD, broşür, kılavuzlar vb. dokümanlar ve montaj aparatları ürünler ile birlikte temin edilmelidir.*
- *Teklif edilen ürünler ve her bir parçası daha önce kullanılmamış olmalı, arızasız ve hasarsız olarak orijinal ambalajı içerisinde, her türlü darbe ve hasara karşı tüm önlemler alınmış olarak gönderilmelidir.*
- *Cihazın görünür bir yerinde imalatçı firma adı, tip, model, seri no, teknik değerler v.s. gösteren bir etiket olacaktır.*
- *Teklif edilecek herhangi bir ürün için End Of Life (EOL)/End Of Sale(EOS) duyurusu yapılmamış olmalıdır.*
- *Teklif edilecek ürün End Of Life (EOL) duyurusu yapıldıktan sonra en az 5 yıl boyunca üretici firma tarafından destek verilmelidir.*
- *Cihazlar ile birlikte teklif edilecek tüm birimler (GBIC, SFP, SFP+, QSFP, Direct Attach Cable vb.) cihaz ile aynı markaya sahip olacak ve OEM ürünler olmayacaktır.*
- *Firmalar, teklif edilen ürün için Yetkili*

indicating that the product is an output of the Authorized Distributor shall be presented during the delivery. • Transportation, insurance, and any related costs including but not limited to courier fees during the warranty period related to the proposed product will be covered by the contractor. • In the case of the failure of any product due to material, workmanship, or assembly errors during the warranty period; the contractor is responsible to repair the product without requesting any payment within 20 working days. If the repair is impossible, the contractor should provide a new product which has the same properties as the failed one within 2 weeks. If this is also impossible the contractor is responsible for providing a new product that has specifications exceeding the failed one with the approval of the end user/beneficiary within one month duration. • All products offered must be covered by a minimum 3-year warranty. This warranty is a manufacturer's warranty and the warranty period shall be initiated after the completion of the inspection and acceptance of the system. Any part of the devices will not be excluded from this warranty for any reason. Due to defects in the guaranteed products during the warranty period, the cargo fees arising from	<i>Distribütör çıkışlı olduğunu gösterir belgeyi teslimatta sunacaklardır.</i> ○ <i>Teklif edilen ürünle ilgili nakliye, taşıma, sigorta ve bunlara bağlı garanti süresindeki kargo ücretleri de dahil olmak üzere ama bununla sınırlı kalmayarak her türlü masraflar yüklenici tarafından karşılanacaktır.</i> ○ <i>Garanti süresi zarfında, gerek malzeme, gerekse işçilik ve montaj hatalarından dolayı arızalanması halinde, herhangi bir ad altında hiçbir ücret talep etmeksizin 20 iş günü içerisinde tamirini, tamiri mümkün değilse aynı ürünün 2 hafta içerisinde yenisini, yenisinin temini mümkün değilse 1 ay içerisinde faydalanıcının onaylayacağı üst model bir ürünü temin etmek zorundadır.</i> ○ <i>Teklif edilen tüm ürünler en az 3 yıl garanti kapsamı içinde olmalıdır. Bu garanti, üretici firma garantisi olup garanti süresi muayene ve kabulün tamamlanmasından sonra başlatılmalıdır. Cihazların hiçbir parçası herhangi bir gerekçeyle bu garantiden ayrı tutulamaz. Garanti kapsamı süresince garantili ürünlerde oluşan arızalardan dolayı ürünlerin servise gidiş ve gelişlerinden doğacak kargo ücreti faydalanıcıdan talep edilmeyecektir.</i>
--	---

the arrival and departure of the products will not be requested from the end user/beneficiary. • The contractor should assign a project manager. The CV of the project manager will be presented after the signing of the contract and will be approved by beneficiary/end user and UNDP. The minimum characteristics of this person are defined below, ○ He/She should be a computer engineer or electrical/electronics engineer. ○ He/She should have at least 3 years of professional experience. ○ He/She should have experience in system room establishment, server and data storage, network and security projects. • Installations of the products must be turnkey and should be accomplished by at least 2 company engineers in order to prevent possible disruptions in the delivery. • Installation of products and inclusion in the system should not give any damage to the existing systems of the end user/beneficiary. • Delivery of products must not exceed 90 days after the contract is signed. • Bidders will add documents which prove their authorization to sell, install and provide warranty and maintenance services for the products from the manufacturers or	○ <i>Firma tarafında çalışacak proje yöneticisi olmalıdır. Söz konusu proje yöneticisinin özgeçmişi, sözleşmenin imzasından sonra ibraz edilecektir. Bu kişi faydalanıcı ve UNDP tarafından onaylanmalıdır. Bu kişinin minimum özellikleri,</i> - <i>Bilgisayar veya elektrik elektronik mühendisi olmalıdır.</i> - <i>En az 3 yıl tecrübeli olmalıdır.</i> - <i>Sistem odası , sunucu ve veri depolama , ağ ve güvenlik projelerinde görev yapmış olmalıdır.</i> ○ <i>Şartnamede geçen ürünler ile ilgili kurulumlar teslimatta aksama olmaması için en az 2 adet firma mühendisi tarafından yapılmalı ve anahtar teslimi olmalıdır.</i> ○ <i>Ürünlerin kurulumu ve sisteme dahil etme işlemi; faydalanıcının mevcut sistemlerine zarar vermeyecek şekilde olmalıdır.</i> ○ <i>Ürünlerin teslimi sözleşme imzalandıktan sonra 90 günü geçmemelidir.</i> ○ <i>Teklif verecek firmalar teklif ettikleri tüm ürünler ile ilgili bu proje için özel olarak üretici firmalardan veya Türkiye resmi distribütörü</i>
--	--

the official distributor companies of Turkey specifically for this project regarding all the products they offer. • In order to ensure system synchronization and integrity, all devices must be compatible with each other within themselves. The contractor is responsible for the supply of all equipment required for system synchronization and no further costs will be charged for this. • All network switches, Wireless Access devices and controllers to be offered must be the same brand in order to avoid compliance problems and to be managed from a single center. • All Server, Data Storage devices, and other system components that will be used for providing the connection between these must be the same brand or a brand of a solution partner in order to avoid compliance problems and to be managed from a single center. • All systems must operate 24/7 without interruption and problems.	<i>firmalardan, ürünleri satmaya, kurmaya ve ürünlerin garanti ve tamir hizmetlerini vermeye yetkili olduklarına dair yetki belgelerini tekliflerine ekleyeceklerdir.</i> ○ <i>Sistem senkronizasyonun ve bütünlüğünün sağlanabilmesi için tüm cihazlar kendi içlerinde birbirleri ile uyumlu olmalıdır. Sistem senkronizasyonu için gerekli olan her türlü ekipmanın temininden yüklenici firma sorumlu olup bunun için ayrıca bir ücret ödemesi talebinde bulunulmayacaktır.</i> ○ <i>Teklif edilecek tüm Ağ anahtarları, Kablosuz Erişim cihazları ve kontrol üniteleri, uyum problemi yaşanmaması ve tek merkezden yönetilebilmesi için aynı marka olmalıdır.</i> ○ <i>Teklif edilecek tüm Sunucu, Veri Depolama cihazları ve bunların bağlantısını sağlayacak diğer sistem bileşenleri, uyum problemi yaşanmaması ve tek merkezden yönetilebilmesi için aynı marka ya da çözüm ortağına ait bir marka olmalıdır.</i> ○ <i>Tüm sistemlerin kesintisiz ve sorunsuz 7/24 çalışması gerekmektedir.</i>
--	---

Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
1. Server // <i>Sunucu</i>		2 pieces // <i>2 adet</i>
Technical Specifications		
1.1	Each processor must support a 64-bit set of commands.	<i>Her bir işlemci 64-bit komut setini desteklemelidir.</i>
1.2	There must be at least 2 physical processors on the server with an operating speed of at least 3.7 GHz.	<i>Sunucu üzerinde en az 2 adet, en az 3.7 GHz çalışma hızında fiziksel işlemci olmalıdır.</i>
1.3	Each processor must have at least 8 cores. The server must have a total of at least 16 cores.	<i>Her bir işlemci en az 8 çekirdekli olmalıdır. Sunucuda toplam olarak en az 16 çekirdek olmalıdır.</i>
1.4	Each processor must have at least 11 MB of cache.	<i>Her bir işlemci üzerinde en az 11 MB önbellek bulunmalıdır.</i>
1.5	Each processor must have at least 2 UPI (Ultra Path Interconnect) connections.	<i>Her bir işlemci en az 2 adet UPI (Ultra Path Interconnect) bağlantı sayısına sahip olmalıdır.</i>
1.6	Each memory used on the server will be PC4, DDR4.	<i>Sunucu üzerinde kullanılan her bir bellek PC4, DDR4 olacaktır.</i>
1.7	There will be at least 384 GB of memory on the server. (each 2666MT/s and at least a capacity of 12*32 GB).	<i>Sunucu üzerinde her biri 2666MT/s, en az 12 adet 32 GB kapasitesinde olan, toplamda en az 384 GB bellek bulunacaktır.</i>
1.8	There will be at least 24 memory slots on the server.	<i>Sunucu üzerinde en az 24 adet bellek yuvası bulunacaktır</i>
1.9	Memory modules will be ECC(Error Check Correction).	<i>Bellek modülleri ECC(Error Check Correction) özelliğinde olacaktır.</i>
1.10	There should be a built-in dual SD card module on the server to be proposed.	<i>Teklif edilecek sunucu üzerinde dahili çift SD kart takılabilen modül bulunmalıdır</i>
1.11	The server must have at least 2 microSDHC/SDXC cards with a capacity of 64 GB provided by the server manufacturer.	<i>Sunucu için en az 2 adet, sunucu üreticisinin sağladığı 64 GB kapasiteli, microSDHC/SDXC kart bulunmalıdır</i>
1.12	Each server must have at least 1 interface to provide remote access and management at 10/100/1000Mbps.	<i>Her bir sunucu üzerinde en az 1 adet 10/100/1000Mbps hızında uzaktan erişim ve yönetim sağlayacak arabirimi olmalıdır.</i>
1.13	Each server must have at least 4 1Gb Base-T and 2 10GB SFP+ Ethernet ports.	<i>Her bir sunucu üzerinde en az 4 adet 1Gb Base-T ve 2 adet 10GB SFP+ ethernet bağlantı noktası bulunmalıdır.</i>
1.14	At least 2 SR SFP+ modules must be supplied with each server. SFP+ modules must be the original product. Equivalent products will not be accepted.	<i>Her bir sunucu ile birlikte en az 2 adet SR SFP+ modül verilmelidir. SFP+ modüller orijinal ürün olmalıdır. Muadil ürünler kabul edilmeyecektir</i>
1.15	Each server must have at least 2 external HBA controllers running as 12Gbps SAS.	<i>Her bir sunucu üzerinde en az 2 adet 12Gbps SAS olarak çalışan harici HBA kontrol birimi bulunmalıdır.</i>
1.16	The PDU and cables required for the server	<i>Sunucu için gerekli PDU ve kablolar birlikte</i>

	will be delivered together without previous use.	<i>daha önce kullanılmamış olarak teslim edilecektir.</i>
1.17	Each server must have at least 2 redundant power supplies, each with a power of 750W, which can be disassembled and installed during operation. At least 2 redundant power supplies, each with 2400W power, should be installed on the server if necessary.	<i>Her bir sunucu üzerinde çalışma esnasında sökülüp takılabilen; en az 2 adet, her biri 750W gücünde yedekli güç kaynağı bulunmalıdır. Sunucu üzerine gerektiğinde en az 2 adet, her biri 2400W gücünde yedekli güç kaynağı takılabilmelidir.</i>
1.18	For each server, fans must be installed with at least 6 redundant and all fan slots of the proposed system that can be disassembled and installed during operation.	<i>Her bir sunucu için, çalışma esnasında sökülüp takılabilen en az 6 adet yedekli ve teklif edilen sistemin tüm fan yuvaları dolu olacak şekilde fanlar takılı bulunmalıdır.</i>
1.19	The server must support Trusted Platform Module 2.0 (TPM 2.0) and be offered with the necessary licenses	<i>Sunucuda Trusted Platform Module 2.0 (TPM 2.0) desteği bulunmalı ve gerekli lisanslar ile teklif edilmelidir</i>
1.20	There must be at least 1 VGA port and 4 USB ports on the server to be offered.	<i>Teklif edilecek sunucu üzerinde en az 1 adet VGA portu, toplam 4 adet USB portu bulunmalıdır.</i>
1.21	There must be at least 1 PCIe Gen3 x16 at least 4 PCIe slots on the server to be offered.	<i>Teklif edilecek sunucu üzerinde en az 1 adedi PCIe Gen3 x16 en az 4 adet PCIe slotu bulunmalıdır.</i>
1.22	Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi operating systems may be installed on the servers.	<i>Sunucular üzerine, Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi işletim sistemleri kurulabilecektir.</i>
1.23	The server to be offered must have a graphics card with at least 16mb of memory and supports a resolution of at least 1920*1200.	<i>Teklif edilecek sunucu üzerinde embedded olarak en az 16mb belleğe sahip ve en az 1920*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.</i>
1.24	At least 6 Single wide or at least 3 Double wide GPU cards can be installed on the server to be offered in necessary cases.	<i>Teklif edilecek sunucu üzerine gerektiğinde en az 6 adet Single wide veya gerektiğinde en az 3 adet Double wide GPU kart takılabilmelidir</i>
1.25	The server must have a lockable front cover to prevent physical interference.	<i>Sunucu üzerinde fiziksel müdahaleleri engelleyebilmek için kilitlenebilir ön kapak bulunmalıdır.</i>
1.26	The files required for system installation on the proposed server must be embedded and the system must be installed through the embedded system without the need for any disk drive.	<i>Teklif edilen sunucu üzerinde sistem kurulumu için gerekli dosyalar embedded olmalıdır ve herhangi bir disk, sürücü ye ihtiyaç olmadan embeded sistem üzerinden sistem kurulabilmelidir.</i>
1.27	The server must have an LCD screen or warning lights showing system name, serial number, remote management IP number, power consumption, and fault information that ensures easy detection of failures.	<i>Sunucu üzerinde sistem ismi, seri numarası, uzaktan yönetim IP numarası, güç tüketimi ve arızaların kolay tespit edilebilmesini sağlayan arıza bilgilerini gösteren LCD ekran ya da uyarı ışıkları bulunmalıdır.</i>
1.28	The server must have a remote	<i>Sunucu üzerinde HTTPS ve SSLv2 sertifika ile</i>

	management module with its own 1 Gb physical port that will provide access with HTTPS and SSLv2 certificates.	<i>erişim sağlayacak kendine ait 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır.</i>
1.29	One of the USB ports on the front panel of the server must be accessible by the remote management port, a firmware update or authorization can be made with the USB memory that can be installed through this port when the server is closed, and the remote management web interface must be accessed by connecting it to a computer by USB cable when the remote management network is not installed or working.	<i>Sunucu ön panelinde bulunan USB portlardan bir adeti uzaktan yönetim portu tarafından erişilebilmeli, sunucu kapalı olduğu esnada bu port üzerinden takılabilecek USB bellek ile firmware güncellemesi veya provizyonlama yapılabilmeli ve uzaktan yönetim networkünün kurulu olmadığı veya çalışmadığı esnada USB kablo ile bir bilgisayara bağlayarak uzaktan yönetim web ara yüzüne erişilebilmelidir.</i>
1.30	The remote management module must have HTML5 support and modern web servers should be managed without installing any agents, plugins, remote KVM access should be made, the operating system should be established by remote media connection and updates should be made.	<i>Uzaktan yönetim modülünün HTML5 desteği olmalı ve herhangi ajan, eklenti yüklenmeden modern web sunucuları yönetilmeli, uzaktan KVM erişimi yapılabilmeli, uzaktan medya bağlantısı yapılarak işletim sistemi kurulabilmeli ve güncellemeler yapılabilmelidir.</i>
1.31	Servers must support virtual media, use USB sticks, CDs, DVDs, etc. connected to a remote computer.	<i>Sunucular sanal medya özelliğini desteklemelidir, uzaktaki bir bilgisayara bağlı USB bellek, CD, DVD, vb. medyaları kullanabilmelidir.</i>
1.32	The remote management module should be able to manage the server RAID card, configure the disks to be added to the server later, and increase its capacity by adding disks to existing RAID groups.	<i>Uzaktan yönetim modülü sunucu RAID kartının yönetimini gerçekleştirebilmeli, sunucuya sonradan eklenecek disklerin RAID yapılandırmasını yapabilmeli ve mevcut RAID guruplarına disk eklemesi yaparak kapasitesini artırılmasını sağlayabilmelidir.</i>
1.33	The server must be able to check the security and authenticity of the BIOS, firmware etc. files to be installed on it through the certificate, and there must be a secure non-volatile memory space on the server that ensures that security certificates are protected against attacks.	<i>Sunucu, üzerine yüklenecek BIOS, firmware vb dosyalarının sertifika vasıtası ile güvenliğini ve orijinalliğini kontrol edebilmeli, sunucu üzerinde, güvenlik sertifikalarının saldırılara karşı korunmasını sağlayan, uçucu olmayan güvenli bir bellek alanı bulunmalıdır.</i>
1.34	There should be a metal alloy sliding rail system with accessories to prevent the proposed server from bending when pressed to ensure that it is pulled forward from the cab during operation.	<i>Teklif edilecek sunucunun çalışma esnasında kabinden öne çekilerek müdahale edilmesini sağlayacak üzerine baskı olduğunda eğilmesini engelleyecek aksesuarlara sahip metal alaşımlı kayan ray sistemi bulunmalıdır.</i>
1.35	The server to be offered must have access and management support via mobile phone or tablet upon request.	<i>Teklif edilecek sunucunun istenildiğinde cep telefonu veya tablet üzerinden erişim ve yönetim desteği olmalıdır.</i>
1.36	All components supplied with the server	<i>Sunucu beraber verilen bütün komponentler</i>

	must be manufactured by the server manufacturer or approved by the server manufacturer and supplied by the server manufacturer and the current configuration of the server must be questioned through a portal belonging to the manufacturer, the server guarantee must cover all components on the server.	<i>sunucu üreticisi tarafından üretilmiş veya sunucu üreticisi tarafından onaylanarak tedariki sunucu üreticisi tarafından yapılmış olmalı ve üreticiye ait bir portal üzerinden sunucunun güncel konfigürasyonu sorgulanabilmeli, sunucu garantisi, sunucu üzerinde gelen bütün komponentleri kapsamalıdır.</i>
1.37	It will operate on the city grid with 220 V AC and 50 Hz single or three-phase energy supply. Feed cable plugs for energy input will be of the appropriate type to the power distribution units in the existing cabinets.	<i>220 V AC ve 50 Hz tek veya üç faz enerji beslemesi ile şehir şebekesinde çalışacaktır. Enerji girişi için besleme kablo fişleri mevcut kabinler içerisindeki güç dağıtım ünitelerine uygun tipte olacaktır.</i>
1.38	Servers will have a manufacturer's warranty on the next business day for at least 3 years. The letter that the warranty is given by the manufacturer should be provided in delivery time.	<i>Sunucular en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır. Garantinin üretici firma tarafından verildiğine dair yazı teslimat sırasında ibraz edilecektir.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
2. Data Storage Unit // <i>Veri Depolama ünitesi</i>		1 piece // <i>1 adet</i>
Technical Specifications		
2.1	The data storage manufacturer to be offered will be the same brand or a brand of a solution partner as the proposed server computers.	<i>Teklif edilecek veri depolama üreticisi, teklif edilen sunucu bilgisayarlar ile aynı marka ya da çözüm ortağı firmanın markası olacaktır.</i>
2.2	The external data storage system to be proposed must not consist of combining multiple data storage systems with clustering or similar methods.	<i>Teklif edilecek harici veri depolama sistemi, birden fazla veri depolama sisteminin kümeleme veya benzeri yöntemlerle birleştirilmesinden oluşmuş olmamalıdır.</i>
2.3	Measures must be taken against a single-point error in the external data storage system to be offered and ensure that the backup unit data storage system operates continuously in case of failure of any part.	<i>Teklif edilecek harici veri depolama sisteminde tek noktadan hata durumuna karşı önlemler alınmış olmalı ve herhangi bir parçanın arızasında yedek birim veri depolama sisteminin durmadan çalışmasını sağlamalıdır.</i>
2.4	In case of any failure in the external data storage system to be proposed, the replacement of any part in the system (disc, power supply, fans, etc.) should be carried out without requiring system shutdown.	<i>Teklif edilecek harici veri depolama sisteminde herhangi bir sorun çıkması durumunda sistem içerisindeki herhangi bir parçanın (disk, güç kaynağı, fanlar, vs.) değiştirilmesi sistem herhangi bir sistem kapanması gerektirmeden yapılabilir.</i>
2.5	There must be two control units (dual controllers) on the external storage system.	<i>Harici depolama sistemi üzerinde iki adet kontrol ünitesi (dual controller) bulunmalıdır.</i>
2.6	The proposed data storage unit must be	<i>Teklif edilen veri depolama ünitesi, 16 Gb FC,</i>

	able to connect the server with 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI, and 12 Gb SAS ports. At least 8 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI, and 12 Gb SAS ports should be installed on the proposed data storage unit as needed. In addition, the data storage unit must support at least 4 16Gb FC and at least 4 10Gb SFP+ ports on the device at the same time if desired (multi-protocol ports).	<i>10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI ve 12 Gb SAS portları ile sunucu bağlantısını sağlayabilmelidir. Teklif edilen veri depolama ünitesi üzerine ihtiyaca göre en az 8 adet 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI ve 12 Gb SAS portları takılabilmelidir. Ayrıca veri depolama ünitesi istenirse en az 4 adet 16Gb FC ve en az 4 adet 10Gb SFP+ portun aynı anda cihaz üzerinde bulunmasını desteklemelidir (multi-protocol ports).</i>
2.7	Each controller will have a total of at least 8 pieces of 12 Gbps SAS ports, including at least 4 SAS ports at a speed of 12 Gbps.	<i>Her kontrol ünitesi (controller) üzerinde 12 Gbps hızında en az 4 adet SAS port olmak üzere toplamda en az 8 adet 12 Gbps SAS port bulunacaktır.</i>
2.8	At least 2 pieces, at least 2 meters long, 12 Gbps, HD Mini-SAS to HD Mini-SAS cable will be supplied with the storage unit. All cables must belong to the storage manufacturer.	<i>Depolama ünitesi ile birlikte en az 2 adet, en az 2 metre uzunluğunda, 12 Gbps, HD Mini-SAS to HD Mini-SAS kablo verilecektir. Tüm kablolar depolama üreticisine ait olmalıdır.</i>
2.9	Each control unit must have a management port with a speed of at least 1Gbps.	<i>Her kontrol ünitesi yönetim için en az 1Gbps hızına sahip yönetim portu bulunmalıdır.</i>
2.10	Each controller on the external disk unit to be offered must have at least 8 GB of memory and a total of 16 GB of memory. This capacity must be dram type. Within the scope of this cache capacity, fields created with SSD/FMD, I/O card will not be accepted.	<i>Teklif edilecek harici disk ünitesi üzerinde bulunan her kontrol ünitesi üzerinde en az 8, toplamda ise 16 GB bellek bulunmalıdır. Bu kapasite DRAM tipinde olmalıdır. Bu önbellek kapasitesi kapsamında SSD/FMD, I/O kart ile oluşturulan alanlar kabul edilmeyecektir.</i>
2.11	Firmware updates should be available without causing disruption to the running system.	<i>Çalışan sistem üzerinde kesinti yaratmadan firmware güncellemeleri yapılabilmelidir.</i>
2.12	The Storage Unit should be able to expand to at least 276 disk capacity with the proposed controllers and grow to at least 3PB capacity.	<i>Depolama Ünitesi, teklif edilen kontrol birimleri ile en az 276 adet disk kapasitesine genişleyebilmeli ve en az 3PB kapasitesine kadar büyüebilmelidir.</i>
2.13	The system disk boost should be incremental in the form of racks and these racks should be manageable with an integrated HTML5 web-based GUI interface. Racks should be able to be created from 24 2.5" disks to provide the total number of discs, and the connection between the racks should be made with a 12 Gbit SAS interface. Each of the shelves should be no more than 2U high.	<i>Sistem disk artırımı raflar şeklinde arttırılabilir olmalı ve bu raflar entegre bir HTML5 web tabanlı GUI arayüzü ile yönetilebilir olmalıdır. Raflar toplam disk sayısını sağlamak üzere 24 adet 2.5" disklerden oluşturulabilmeli ve raflar arasındaki bağlantı 12 Gbit hızında SAS arayüz ile yapılmalıdır. Rafların her biri en fazla 2U yükseklikte olmalıdır.</i>
2.14	The system must have at least 12 SSD drives with a connection speed of 12Gbps, ssd technology with a capacity of 960 GB, and	<i>Sistem üzerinde en az 12 adet, 12Gbps bağlantı hızında, 960 GB kapasiteli SSD teknolojisi diskler ve en az 12 adet 10000</i>

	SAS disks with a capacity of 1.8 TB with a rotational speed of at least 12 10000 RPM.	<i>RPM dönüş hızında, 1.8 TB kapasiteli SAS diskler bulunmalıdır.</i>
2.15	The disks used must be high-performance SAS, NL-SAS, SSD, and FIPS certified self-encrypting SAS and SSD in accordance with the selected disc racks.	<i>Kullanılan diskler seçilen disk raflarına uygun şekilde yüksek performanslı SAS, NL-SAS, SSD ve FIPS sertifikalı self-encrypting SAS ve SSD olabilmelidir.</i>
2.16	The proposed data storage system must monitor the I/O that each disk makes, proactively monitor the health status performance graph, and work to provide the necessary warnings before the disk fails. Systems that fail to provide this must offer 30% additional capacity.	<i>Teklif edilen veri depolama sistemi her disk in yaptığı I/O yu izlemeli sağlık durumunu performans grafiğini proaktif olarak izlemeli ve disk bozulmadan önce gerekli uyarıları verecek şekilde çalışmalıdır. Bunu sağlayamayan sistemler %30 ilave kapasite verecek şekilde teklif etmelidirler.</i>
2.17	The system must have Distributed RAID or similar technology that reduces rebuild times when disk failures occur on it.	<i>Sistem, üzerinde disk arızaları meydana geldiği zaman, yeniden oluşturma sürelerini azaltan Distributed RAID veya benzeri bir teknolojiye sahip olmalıdır.</i>
2.18	The system should be able to support at least 64 host connections with a fiber connection option.	<i>Sistem Fiber bağlantı seçeneği ile en az 64 adet host bağlantısını destekleyebilmelidir.</i>
2.19	The external disk system must support RAID levels 0, 1, 5, 6, and 10. Alternative data protection methods will not be accepted.	<i>Harici disk sistemi 0, 1, 5, 6 ve 10 RAID seviyelerini desteklemelidir. Alternatif veri koruma yöntemleri kabul edilmeyecektir.</i>
2.20	Additions should be made to the virtual disk groups being used in the system without interruption of access.	<i>Sistemde kullanılmakta olan sanal disk gruplarına erişim kesintisi olmadan ilaveler yapılabilirdir.</i>
2.21	All licenses supported by the data storage unit (snapshot, clone, read cache, auto-tiering, replication, etc.) must be offered together with the proposed data storage unit in order to avoid additional costs at a later date.	<i>Teklif edilen veri depolama ünitesi ile birlikte ileri tarihlerde ek maliyet olmaması açısından, veri depolama ünitesinin desteklediği tüm lisanslar (snapshot, clone, read cache, auto tiering, replikasyon vb.) ile birlikte teklif edilmelidir.</i>
2.22	The proposed data storage system should support the use of SSDs, which can be added to the system if desired, as a read-cache. SSD cache capacity can be raised up to 4TB. If there is an additional license requirement for this feature, it must be included in the offer.	<i>Teklif edilecek veri depolama sistemi, istendiği takdirde sisteme eklenebilecek SSD'lerin okuma ve yazma amaçlı önbellek olarak kullanımını desteklemelidir. SSD önbellek kapasitesi 4TB'a kadar yükseltilebilmelidir. Bu özellik için ek bir lisans gereksinimi varsa teklife dahil edilmelidir.</i>
2.23	The data storage system to be offered must have automatic data tiering that supports at least 3 layers (SSD, SAS, NL-SAS/SATA). By monitoring data activities on storage areas at the sub-LUN level, the data storage system should be able to automatically move heavily used sub-logical areas to faster storage and underused sub-logical areas to slower storage (automatic data	<i>Teklif edilecek veri depolama sistemi, en az 3 katmanı (SSD, SAS, NL-SAS/SATA) destekleyen otomatik veri katmanlandırma özelliğine sahip olmalıdır. Veri depolama sistemi, depolama alanları üzerindeki veri aktivitelerini alt mantıksal alan (sub-LUN – blok) seviyesinde izleyerek, yoğun kullanılan alt mantıksal alanları daha hızlı depolama alanına ve az kullanılan alt mantıksal alanları</i>

	tiering). Within the scope of this property, the data must be in the form of moving movements between layers, not in the form of copying. If a license is required to provide such a feature, the required licenses will be included in the offer for the maximum capacity supported by the system.	<i>daha yavaş depolama alanına otomatik olarak taşıyabilmelidir (otomatik veri katmanlandırma). Bu özellik kapsamında verilerin katmanlar arasındaki hareketleri taşıma şeklinde olmalı, kopyalama şeklinde olmamalıdır. Söz konusu özelliğin sağlanabilmesi için lisans gerekmesi durumunda, gerekli olan lisanslar, sistemin desteklediği maksimum kapasite için teklife dahil edilecektir.</i>
2.24	The proposed data storage unit must support "thin provisioning".	<i>Teklif edilen veri depolama ünitesi "thin provisioning" desteği olmalıdır.</i>
2.25	At least 512 (five hundred) LUNs must be created in the proposed data storage unit.	<i>Teklif edilen veri depolama ünitesinde en az 512 (beşyüz) LUN yaratılabilir.</i>
2.26	The external data storage system to be offered must be able to receive snapshots and full copies (clones) and return them (restored). The licenses required for this feature will be added to the offer for the maximum capacity supported by the system.	<i>Teklif edilecek harici veri depolama sistemi snapshot (anlık kopya) ve tam kopya (clone) alabilmeli ve bu kopyalardan geri dönebilmelidir (restore). Bu özellik için gerekli lisanslar sistemin desteklediği maksimum kapasite için teklife eklenecektir.</i>
2.27	The external data storage system to be offered should use the ROW (Redirect on Write) method and not the COW (Copy on Write) method to avoid affecting the snapshot. Working principles will be documented with manufacturer's documents.	<i>Teklif edilecek harici veri depolama sistemi anlık kopyalama (snapshot) performansını etkilememesi için ROW (Redirect on Write) metodunu kullanmalı, COW (Copy on Write) metodunu kullanmamalıdır. Çalışma prensipleri üretici dokümanları ile belgelenmelidir.</i>
2.28	The proposed data storage unit must support at least 1024 snapshots.	<i>Teklif edilen veri depolama ünitesinin en az 1024 adet snapshot desteği olmalıdır.</i>
2.29	The external data storage system to be offered is asynchronous, it must support replication. If additional hardware and licenses are required for this feature, it must be added to the offer for maximum capacity.	<i>Teklif edilecek harici veri depolama sistemi asenkron, replikasyonu desteklemelidir. Bu özellik için ek donanım ve lisans gerekiyorsa teklife maksimum kapasite için eklenmelidir.</i>
2.30	The proposed data storage unit must have at least 2 redundant power supply with a power of at least 580 Watts. 2 power cables must be supplied with the data storage unit.	<i>Teklif edilen veri depolama ünitesi en az 2 adet, en az 580 Watt gücünde yedekli güç kaynağına (redundant power supply) sahip olmalıdır. Veri depolama ünitesi ile birlikte 2 adet güç kablosu verilmelidir.</i>
2.31	External disk unit must support at least VMware 6.0, 6.5, and 6.7; Windows Server 2012, 2016,2019, RHEL 6.0, and 7.4 SLES 12.3 operating systems.	<i>Harici disk ünitesi en az VMware 6.0, 6.5 ve 6.7; Windows Server 2012, 2016,2019, RHEL 6.0 ve 7.4, SLES 12.3 işletim sistemlerini desteklemelidir.</i>
2.32	The external disk volume must support VMware vSphere (ESXi), Microsoft Hyper-V,	<i>Harici disk ünitesinin VMware vSphere (ESXi), Microsoft Hyper-V ve vCenter SRM desteği</i>

	and vCenter SRM.	<i>olmalıdır.</i>
2.33	Data Storage system management should be web-based without the need to install additional software.	<i>Veri Depolama sisteminin yönetimi ek bir yazılım yüklemeye gerek kalmadan web tabanlı olarak yapılabilmelidir.</i>
2.34	The external data storage system to be offered will have the ability to alert the system administrator by e-mail in case of a failure on it.	<i>Teklif edilecek harici veri depolama sistemi, üzerinde oluşan bir arıza durumunda sistem yöneticisini e-posta ile uyarma özelliğine sahip olacaktır.</i>
2.35	The data storage unit should have a next-day guarantee of the manufacturer for at least 3 years.	<i>Veri depolama ünitesi en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
3. Virtualization Software // <i>Sanallaştırma Yazılımı</i>		1 piece // <i>1 adet</i>
Technical Specifications		
3.1.	Virtualization software will be licensed for a total of 6 CPUs.	<i>Sanallaştırma yazılımı toplam 6 CPU için lisanslandırılacaktır.</i>
3.2.	The proposed virtualization software must allow over-commitment of virtual machines to be created on the same physical server above existing system resources.	<i>Teklif edilen sanallaştırma yazılımı aynı fiziksel sunucu üzerinde oluşturulacak sanal makinelerin mevcut sistem kaynaklarının üzerinde kaynak atanmasına (over-commitment) izin vermelidir.</i>
3.3.	The proposed virtualization software must support SMP (Symetric Multi Processing). In the proposed system, 128 virtual CPUs should be assigned to each virtual machine at any time.	<i>Teklif edilen sanallaştırma yazılımı SMP (Symetric Multi Processing) desteği olmalıdır. Teklif edilen sistemde her bir sanal makineye istenildiğinde 128 adet sanal CPU atanabilmelidir.</i>
3.4.	With the proposed virtualization software, 1TB of virtual memory should be assigned to each virtual machine.	<i>Teklif edilen sanallaştırma yazılımı ile her bir sanal makineye 1TB sanal bellek atanabilmelidir.</i>
3.5.	The proposed virtualization software should be able to enlarge the virtual machine disk as it fills up, instead of retrieving the assigned disk space for each virtual machine directly from the disk pool. (Thin Provisioning)	<i>Teklif edilen sanallaştırma yazılımı gerektiğinde her bir sanal makine için atanan disk alanın doğrudan disk havuzundan almak yerine, sanal makine diski doldukça büyütebilmelidir. (Thin Provisioning)</i>
3.6.	The proposed virtualization software guest operating system "GuestOS" must support current versions of Windows 8, Windows 10, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, SUSE Linux, Debian, Oracle Linux, MacOSX, FreeBSD operating systems.	<i>Teklif edilen sanallaştırma yazılımı misafir işletim sistemi "Guest OS" olarak, Windows 8, Windows 10, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, SUSE Linux, Debian, Oracle Linux, MacOSX, FreeBSD işletim sistemlerinin güncel versiyonlarını desteklemelidir.</i>

3.7.	The proposed virtualization software must allow the file system containing the disks and virtual machines given to virtual machines to be enlarged while the system is running.	<i>Teklif edilen sanallaştırma yazılımı, sanal makinalara verilen disklerin ve sanal makinaların bulunduğu dosya sisteminin sistem çalışırken büyütülmesine izin vermelidir.</i>
3.8.	The proposed virtualization software should enable the assignment of 62 TB virtual disks to virtual machines.	<i>Teklif edilen sanallaştırma yazılımı sanal makinalara 62 TB boyutunda sanal diskler atanmasına olanak sağlamalıdır.</i>
3.9.	Proposed virtualization software must be able to manage 64 TB of storage	<i>Teklif edilen sanallaştırma yazılımı 64 TB boyutundaki depolama alanlarını yönetebilmelidir</i>
3.10.	Support data storage technologies such as FC, iSCSI, and NFS and data storage units that work with these technologies with the proposed virtualization software.	<i>Teklif edilen sanallaştırma yazılımı ile FC, iSCSI ve NFS gibi veri depolama teknolojilerini ve bu teknolojilerle çalışan veri depolama ünitelerini desteklemelidir.</i>
3.11.	With the proposed virtualization software, authorization should be made in the system, allowing certain operational persons to access the entire virtual system or part of the virtual system and carry out management operations.	<i>Teklif edilen sanallaştırma yazılımı ile sistemde yetkilendirme yapılabilmesi, belirli operasyonel kişilerin tüm sanal sisteme veya sanal sistemin bir kısmına erişmelerine ve yönetim operasyonlarını gerçekleştirebilmelerine imkan tanımalıdır.</i>
3.12.	With the proposed virtualization software, system performance should be monitored instantly or retrospectively for parameters such as CPU, memory, disk, and network, and a report should be obtained.	<i>Teklif edilen sanallaştırma yazılımı ile sistem performansı CPU, memory, disk ve network gibi parametreler için anlık veya geçmişe doğru izlenebilmeli, rapor alınabilmelidir.</i>
3.13.	The proposed virtualization software must include centralized management software that enables the management of all virtual servers from a single center. The management software will be the full version. (Will be offered with centralized management software licenses)	<i>Teklif edilen sanallaştırma yazılımı tüm sanal sunucuların tek bir merkezden yönetimini sağlayan merkezi yönetim yazılımını içermelidir. Yönetim yazılımı tam sürüm olacaktır. (Merkezi yönetim yazılımı lisansları ile teklif edilecektir)</i>
3.14.	The centralized management software that comes with the proposed virtualization software must be connected and managed from the web interface.	<i>Teklif edilen sanallaştırma yazılımı ile gelen merkezi yönetim yazılımı web arayüzünden bağlanıp yönetmeye olanak sağlamalıdır.</i>
3.15.	The proposed virtualization software must allow VLAN assignment to virtual servers.	<i>Teklif edilen sanallaştırma yazılımı sanal sunuculara VLAN atanmasına izin vermelidir.</i>
3.16.	The proposed virtualization software must allow a copy of the virtual servers to be made while they are open.	<i>Teklif edilen sanallaştırma yazılımı sanal sunucuların açıkken bir kopyasının çıkarılmasına izin vermelidir.</i>

3.17.	The proposed virtualization software should be able to transfer running virtual machines to another server within the virtualization system without the need for shared disk space when needed and perform this process for multiple virtual machines at the same time.	<i>Teklif edilen sanallaştırma yazılımı çalışan durumdaki sanal makinaları ihtiyaç duyulduğunda paylaşımlı bir disk alanına ihtiyaç duymaksızın sanallaştırma sistemi içindeki başka bir sunucuya aktarabilmeli, bu işlemi aynı anda birden fazla sanal makina için gerçekleştirebilmelidir.</i>
3.18.	There should be clustering service support in the form of automatic operation of virtual machines that shut down when there is an out-of-control stop on one of the servers defined in the proposed virtualization software. This service should be prioritized between virtual machines.	<i>Teklif edilen sanallaştırma yazılımı içerisinde tanımlı sunuculardan birisinde kontrol dışı bir duruma olduğunda kapanan sanal makinaların sistemdeki diğer sunucular tarafından otomatik olarak çalıştırılması şeklinde kümeleme hizmeti desteği olmalıdır. Bu hizmet için sanal makinalar arasında önceliklendirme yapılabilmelidir.</i>
3.19.	The proposed virtualization software must include a module that takes backups of Windows and Linux virtual machines running into the disk environment. This module should be able to store backed-up data by singularization.	<i>Teklif edilen sanallaştırma yazılımı içerisinde çalışan Windows ve Linux sanal makinaların yedeklerini disk ortamına alan bir modülü bulunmalıdır. Bu modül yedeklenmiş verileri tekilleştirme yaparak saklayabilmelidir.</i>
3.20.	The proposed virtualization software should allow designated virtual machines to replicate on virtualization servers in the same location or remote location.	<i>Teklif edilen sanallaştırma yazılımı belirlenen sanal makinaların aynı lokasyondaki veya uzak bir lokasyondaki sanallaştırma sunucuları üzerine replikasyon yapmasına olanak tanımalıdır.</i>
3.21.	The proposed virtualization software should be able to work integrated with third-party antivirus solutions and enable virus scanning on virtual machines using agency-independent architecture.	<i>Teklif edilen sanallaştırma yazılımı üçüncü parti antivirus çözümleri ile entegre çalışabilmeli ve ajansız mimari kullanarak sanal makinalar üzerinde virüs taraması yapılmasına olanak sağlamalıdır.</i>
3.22.	The proposed virtualization software must be able to move working virtual machines between their disks and storage areas.	<i>Teklif edilen sanallaştırma yazılımı çalışan durumdaki sanal makinaları diskleri ile birlikte depolama alanları arasında taşıyabilmelidir.</i>
3.23.	The proposed virtualization software must support the addition of CPU, memory, disk, and network cards to running virtual machines.	<i>Teklif edilen sanallaştırma yazılımı çalışan durumdaki sanal makinalara CPU, memory, disk ve network kartı eklenmesini desteklemelidir.</i>
3.24.	The proposed virtualization software should be able to ensure that the physical servers it operates for the selected virtual machines continue to operate from other physical servers without interruption in the event of an unplanned outage.	<i>Teklif edilen sanallaştırma yazılımı seçilen sanal makinalar için çalıştığı fiziksel sunucuların plansız bir kesinti yaşaması durumunda, kesintisiz olarak diğer fiziksel sunuculardan çalışmasına devam etmesini sağlayabilmelidir.</i>

3.25.	Performance monitoring software should be able to monitor performance according to disk, memory, CPU, and network resources.	<i>Performans izleme yazılımı disk, bellek, cpu ve network kaynaklarına göre performans izlemesi yapabilmelidir.</i>
3.26.	Performance monitoring software should be able to automatically make adaptive threshold definitions for resource usage by learning the system resource usage curve and be able to sound the alarm when resource usage rises below or above this lower threshold.	<i>Performans izleme yazılımı sistem kaynak kullanım eğrisini öğrenerek otomatik olarak kaynak kullanımı için adaptif eşik tanımlamaları yapabilmeli ve kaynak kullanımını bu alt eşğin altına veya üst eşğin üstüne çıktığında alarm verebilmelidir.</i>
3.27.	Performance monitoring software should be able to detect incidents that may cause performance problems by associating alarms, errors, or warnings in the system with source usage graphs when necessary.	<i>Performans izleme yazılımı gerektiğinde sistemdeki alarm, hata veya uyarıları kaynak kullanım grafikleri ile ilişkilendirerek performans sorununa neden olabilecek olayları tespit edebilmelidir.</i>
3.28.	Performance monitoring software must have its own database, not need a third-party database.	<i>Performans izleme yazılımı kendi veritabanına sahip olmalı, üçüncü parti bir veritabanına ihtiyaç duymamalıdır.</i>
3.29.	Performance monitoring software should be able to monitor all virtual machines in the system to check whether the amounts of resources assigned to virtual machines are correct and to make improvements in this regard.	<i>Performans izleme yazılımı sistemdeki tüm sanal makinaları izleyerek sanal makinalara atanan kaynak miktarlarının doğru olup olmadığını kontrol edebilmeli, bu konuda iyileştirmeler yapabilmek için tavsiyelerde bulunabilmelidir.</i>
3.30.	All software updates and security patches that will be issued for at least 3 years with licenses for the proposed solution must be installed, as well as 5 days and 9 hours of support for 3 years.	<i>Teklif edilen çözüme ait lisanslar ile birlikte en az 3 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 3 yıl boyunca 5 gün 9 saat destek hizmeti verilmelidir.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
4. Backup Software // <i>Yedekleme Yazılımı</i>		1 piece // <i>1 adet</i>
Technical Specifications		
4.1.	The software must be able to back up virtual machines running on the Microsoft Hyper-V and VMware vSphere virtualization platform to the application-consistent image-based disk.	<i>Yazılım Microsoft Hyper-V ve Vmware vSphere sanallaştırma platformunda çalışan sanal makinaların uygulama tutarlı imaj tabanlı diske yedeklemesini yapabilmelidir.</i>
4.2.	The software's management console must be able to work on any physical	<i>Yazılımın yönetim konsolu 64-bit bir Microsoft Windows işletim sistemine sahip</i>

	or virtual, server, or personal computer with a 64-bit Microsoft Windows operating system.	<i>herhangi bir fiziksel veya sanal, sunucu veya kişisel bilgisayar üzerinde çalışabilmelidir.</i>
4.3.	The software must be licensed on the basis of the physical processor of the main servers running the virtual machines that are protected (backed up and/or replicated). There should be no licensing model based on the number of Virtual Machines, disk capacities, and application agents.	<i>Yazılımın lisanslaması korunmakta (yedeklenmekte ve/veya replike edilmekte) olan sanal makineleri çalıştıran ana sunucuların fiziksel işlemcisi bazında olmalıdır. Sanal Makina sayısı, disk kapasiteleri ve uygulama ajanlarına göre bir lisanslama modeli olmamalıdır.</i>
4.4.	In order to improve the backup and replication performance of the Software, the number of structural components such as consoles, proxics, and storage areas should be increased without the need for an additional license.	<i>Yazılımın yedekleme ve replikasyon performansını arttırmak amacı ile konsol, proksi ve depolama alanları gibi yapısal bileşenlerinin sayısı ilave bir lisans gerektirmeden artırılabilir.</i>
4.5.	The Software must be able to use Windows, Linux, CIFS/SMB file shares, and devices that offer singularization to store backed-up virtual machines.	<i>Yazılım, yedeklenen sanal makineleri saklamak için Windows, Linux, CIFS/SMB dosya paylaşımlarını ve tekilleştirme sunan cihazları kullanabilmelidir.</i>
4.6.	The software must use the Changing Block Tracking (CBT) feature offered by hypervisors for incremental backups.	<i>Yazılım artımlı yedekler için hipervizörlerin sunduğu Değişen Blok Takibi (CBT) özelliğini kullanmalıdır.</i>
4.7.	The Software must provide backup options over the Direct Data Storage network, over the Network, or through the Hypervisor I/O platform when reading backups from the source.	<i>Yazılım yedekleri kaynaktan okurken Doğrudan Veri Depolama ağı üzerinden, Ağ üzerinden veya Hipervizör I/O platformu üzerinden yedekleme seçenekleri sunmalıdır.</i>
4.8.	The Software must provide internal command-line (PowerShell) Support.	<i>Yazılım dahili komut satırı (PowerShell) Desteği sunmalıdır.</i>
4.9.	The software must provide a file management interface that will allow file transfer between the main server and other servers and computers.	<i>Yazılım ana sunucu ve diğer sunucu ve bilgisayarlar arasında dosya transferini sağlayacak bir dosya yönetim arayüzü sunmalıdır.</i>
4.10.	The software must provide the ability to move virtual machines over the main server and disk areas. It should be able to do this using VMware vMotion, Storage vMotion, and/or its own transport technology.	<i>Yazılım sanal makineleri ana sunucu ve disk alanları üzerinde taşıma özelliği sunmalıdır. Bu işlemi VMware vMotion, Storage vMotion ve/veya kendi taşıma teknolojisini kullanarak yapabilmelidir.</i>
4.11.	The Software must offer internal compression and singularization that can be customized or disabled by the user without the need for any agent installation.	<i>Yazılım herhangi bir ajan kurulumu gerektirmeden kullanıcı tarafından özelleştirilebilen veya devre dışı bırakılabilen dahili sıkıştırma ve tekilleştirme sunmalıdır.</i>

4.12.	The Software should provide the option to receive fast incremental backups for only one Virtual Machine from a backup task with more than one Virtual Machine in it.	<i>Yazılım, içerisinde birden fazla Sanal Makina bulunan bir backup görevi içerisinde sadece bir Sanal Makina için hızlı artımlı yedek alabilme seçeneği sunmalıdır.</i>
4.13.	The software must offer a single full and subsequent 'continuously incremental' backup, eliminating the need for a periodic full backup.	<i>Yazılım tek bir tam ve sonrasında 'sürekli artımlı' yedekleme sunarak periyodik full yedek alma ihtiyacını ortadan kaldıracak sentetik tam yedekleme sunmalıdır.</i>
4.14.	The Software must be able to automatically copy all backups taken to a disk space or backups of selected Virtual Servers from within for the purpose of copying the backup to a second disk space or for long-term archiving purposes.	<i>Yazılım bir disk alanına alınmış yedeklerin tamamını veya içerisinde seçilen Sanal Sunucuların yedeklerini ikinci bir disk alanına yedeğin kopyalanması veya uzun dönem arşivlenmesi amacı ile otomatik olarak kopyalayabilmelidir.</i>
4.15.	The Software must be able to access backups taken to a disk space, files from Windows or Linux servers to tape units, tape libraries, and Virtual Tape Libraries.	<i>Yazılım bir disk alanına alınmış yedekleri, Windows veya Linux sunucular içerisinde dosyaları teyp ünitelerine, teyp kütüphanelerine ve Sanal Teyp Kütüphanelerine arşivleyebilmelidir.</i>
4.16.	The Software must be able to identify the Cloud disk service offered by a manufacturer-approved service provider as a backup store where backups will be stored and use this space to store backups or copies of backups.	<i>Yazılım üretici onaylı bir servis sağlayıcı tarafından sunulan Bulut disk hizmetini, yedeklerin saklanacağı bir yedek deposu olarak tanımlayabilmeli ve bu alanı yedekleri veya yedeklerin kopyalarını saklama amaçlı kullanabilmelidir.</i>
4.17.	The software must be able to encrypt stored backups and network traffic end-to-end (when transferring, transferring, and storing) AES256bit.	<i>Yazılım saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES256bit şifreleyebilmelidir.</i>
4.18.	The Software should be able to fully back up Virtual Machine, vApp, and metadata directly through the VMware vCloud Director structure and restore the same components to their original location or on a different vCloud Director structure.	<i>Yazılım VMware vCloud Director yapısı üzerinden Sanal Makina, vApp ve metadata'ları doğrudan tam yedekleyebilmeli ve aynı bileşenleri orjinal yerlerine ya da farklı bir vCloud Director yapısı üzerine geri yükleyebilmelidir.</i>
4.19.	The software must be able to perform application-consistent image-based replication of virtual machines running on the Microsoft Hyper-V and VMware vSphere virtualization platform.	<i>Yazılım Microsoft Hyper-V ve VMware vSphere sanallaştırma platformunda çalışan sanal makinelerin uygulama tutarlı imaj tabanlı replikasyonunu yapabilmelidir.</i>
4.20.	The Software must be able to operate the Virtual Server replicated on a master server from the desired return point with predefined Virtual Network	<i>Yazılım bir ana sunucu üzerine replike edilmiş Sanal Sunucuyu istenilen geri dönüş noktasından, önceden tanımlanmış Sanal Ağ ayarları ile çalışır duruma getirebilmelidir.</i>

	settings.	
4.21.	The Software must be able to operate the Virtual Machine with the Microsoft Windows operating system replicated on a master server from the desired return point with predefined IP settings.	<i>Yazılım bir ana sunucu üzerine replike edilmiş Microsoft Windows işletim sistemine sahip Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış IP ayarları ile çalışır duruma getirebilmelidir.</i>
4.22.	The software should be able to replicate from the received backups and create the replication fallback points from the backup files.	<i>Yazılım alınan yedeklerden replikasyon yapabilmeli, replikasyon geri dönüş noktalarını yedek dosyalarından oluşturabilmelidir.</i>
4.23.	The software must provide Planned Transport to organize data center migration without data loss. Virtual Servers within the scope of the plan should be automatically closed in the specified order and the changes should be transferred and made operational in the new location.	<i>Yazılım veri kaybı olmadan veri merkezi taşımalarını organize edecek Planlı Taşıma özelliği sunmalıdır. Plan kapsamındaki Sanal Sunucular belirtilen sıraya göre otomatik olarak kapatılmalı, değişiklikler aktararak yeni lokasyonda çalışır hale getirilmelidir.</i>
4.24.	The software must be able to make a virtual machine operational without the need for additional copying or intervention directly from the full or incremental backup file on the disk.	<i>Yazılım bir sanal makinayı doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.</i>
4.25.	The software must be able to restore a virtual machine from its full or incremental backup file to its original location or on another master server.	<i>Yazılım bir sanal makinayı tam veya artımlı yedek dosyasından orjinal yerine veya başka bir ana sunucu üzerine geri yükleyebilmelidir.</i>
4.26.	When restoring a virtual machine from backup, the software should offer quick recovery by simply transferring the changing blocks.	<i>Yazılım bir sanal makinayı yedekten geri yüklerken sadece değişen blokları aktararak hızlı kurtarma özelliği sunmalıdır.</i>
4.27.	The software must be able to restore the files of a virtual machine on the main server.	<i>Yazılım bir sanal makinanın ana sunucu üzerindeki dosyalarını geri yükleyebilmelidir.</i>
4.28.	The software must be able to independently restore the selected virtual disks of a virtual machine.	<i>Yazılım bir sanal makinanın seçilen sanal diskleri bağımsız olarak geri yükleyebilmelidir.</i>
4.29.	The Software must be able to restore the Complete Virtual Machine, a file from within the virtual machine, Microsoft Exchange, Active Directory, SharePoint application elements, and Microsoft SQL Databases from within snapshots on the HP 3PAR StoreServ, HP StoreVirtual VSA, and NetApp Data ONTAP-based NetApp FAS, NetApp	<i>Yazılım HP 3PAR StoreServ, HP StoreVirtual, HP StoreVirtual VSA ile NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge ve IBM N Serisi Veri Depolama ünitelerinin üzerindeki Snapshot'ların içerisinde Komple Sanal Makinayı, Sanal makinanın içinden bir dosyayı, Microsoft Exchange, Active Directory, SharePoint uygulama öğelerini ve</i>

	FlexArray (V-Series), NetAppData ONTAP Edge, and IBM N Series Data Storage units.	<i>Microsoft SQL Veri tabanlarını geri yükleyebilmelidir.</i>
4.30.	The Software Application must be able to create a second backup on top of NetApp Data ONTAP-based NetApp FAS, NetApp FlexArray (V-Series), NetAppData ONTAP Edge VSA, and IBM N Series Data Storage using consistent NetApp Hardware Snapshots.	<i>Yazılım Uygulama tutarlı NetApp Donanımsal Snapshot'larını kullanarak NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge VSA ve IBM N Serisi Veri Depolama ünitelerinin üzerine ikinci bir yedek oluşturabilmelidir.</i>
4.31.	The software must be able to export groups, users, and computer accounts from within Microsoft Active Directory backups in LDIFDE format.	<i>Yazılım Microsoft Active Directory yedekleri içerisinden grupları, kullanıcıları ve bilgisayar hesaplarını LDIFDE formatında dışarı aktarabilmelidir.</i>
4.32.	The Software must provide the ability to quickly search, find, .msg, or export e-mail items, contacts, or notes, including those permanently deleted from Microsoft Exchange 2010 and 2013 server backups, as files or email attachments with the .pst extension.	<i>Yazılım Microsoft Exchange 2010 ve 2013 sunucu yedekleri içerisinden kalıcı olarak silinmiş olanlar dahil e-posta, takvim ögesi, kişi veya notları hızlıca arama, bulma, .msg veya .pst uzantılı dosya veya eposta eklentisi olarak dışı aktarma olanağı sunulmalıdır.</i>
4.33.	The Software Microsoft SharePoint 2010 and 2013 server backups must provide the ability to quickly search, find, file, or export items and content as a file or email attachments.	<i>Yazılım Microsoft SharePoint 2010 ve 2013 sunucu yedekleri öğeleri ve içerikleri hızlıca arama, bulma, dosya veya eposta eklentisi olarak dışarı aktarma olanağı sunulmalıdır.</i>
4.34.	The software must be able to restore databases from microsoft sql server backups to the local database server	<i>Yazılım Microsoft SQL Sunucu yedekleri içerisinden veritabanlarını yerel veritabanı sunucusuna geri yükleyebilmelidir</i>
4.35.	The software should be able to integrate into the vSphere Web Client, instant-speed backups should be started here, information such as the status of the backups, unprotected virtual machines should be accessible directly from within the web client.	<i>Yazılım vSphere Web Client'a entegre olabilmeli, anlık hızlı yedeklemeler buradan başlatılabilmeli, yedeklerin durumları, korunmayan sanal makineler gibi bilgilere doğrudan web client içerisinden erişilebilmelidir.</i>
4.36.	The Software should be able to import its configuration backup into defined disk space without any user intervention and be restored to include all settings and definitions.	<i>Yazılım kendi konfigürasyon yedeğini herhangi bir kullanıcı müdahalesi gerekmeden tanımlı disk alanına alabilmeli ve tüm ayarları ve tanımlamaları içerecek şekilde geri yüklenebilmelidir.</i>
4.37.	The software must be licensed for the main server environment consisting of 4 physical processors in the environment.	<i>Yazılım ortamdaki 4 fiziksel işlemciden oluşan ana sunucu ortamı için lisanslanmalıdır. işlemci üzerindeki çekirdek (core) sayısı lisans sayısını etkilememelidir.</i>

Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
5. Server Software // <i>Sunucu Yazılımı</i>		1 piece // 1 adet
Technical Specifications		
5.1.	At least 80 core Windows Server 2019 Standard licenses or equivalent must be issued with the proposed servers.	<i>Teklif edilen sunucularla birlikte en az 80 core Windows Server 2019 Standart lisansı ya da eşdeğeri verilmelidir.</i>
5.2.	At least 20 Windows Server 2019 Cal licenses or equivalent must be issued with the proposed servers.	<i>Teklif edilen sunucularla birlikte en az 20 adet Windows Server 2019 Cal lisansı ya da eşdeğeri verilmelidir.</i>
5.3.	At least 2 SQL Server 2019 Standard Edition licenses or equivalent must be issued with the proposed servers.	<i>Teklif edilen sunucularla birlikte en az 2 adet SQL Server 2019 Standard Edition lisansı ya da eşdeğeri verilmelidir</i>
5.4.	At least 20 SQL Server 2019 Cal licenses or equivalent must be issued with the proposed servers.	<i>Teklif edilen sunucularla birlikte en az 20 adet SQL Server 2019 Cal lisansı ya da eşdeğeri verilmelidir.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
6. Backup Unit // <i>Yedekleme Ünitesi</i>		1 piece // 1 adet
Technical Specifications		
6.1.	The product to be offered will be the storage unit NAS device that can be connected to the network.	<i>Teklif edilecek ürün ağa bağlanabilen depolama ünitesi NAS cihazı olacaktır.</i>
6.2.	The data backup unit to be offered will be rack-type attachable to rack cabinets.	<i>Teklif edilecek veri yedekleme ünitesi raf tipinde rack kabinlerine takılabilir yapıda olacaktır.</i>
6.3.	The proposed product must have at least 8 3.5" disc slots. With the addition of disc drawers, 20 3.5" disc slots should be able to be accessed.	<i>Teklif edilen üründe en az 8 adet 3,5" disk yuvası bulunmalıdır. Disk çekmecesini ilavesi ile 20 adet 3,5" disk yuvasına çıkabilmelidir.</i>
6.4.	The proposed product must support 108 TB disk capacity.	<i>Teklif edilen ürün 108 TB disk kapasitesini desteklemelidir.</i>
6.5.	With the proposed product, specially manufactured discs will be supplied for AT least 8 NAB capacity 7200 rpm return speed SATA or NL-SAS type NAS devices.	<i>Teklif edilen ürünle birlikte en az 8 adet en az 8 TB kapasiteli 7200 rpm dönüş hızında SATA veya NL-SAS tipinde NAS cihazları için özel üretilmiş diskler verilecektir.</i>
6.6.	The system memory of the proposed product must be at least 2 GB of DDR3. With the addition of the memory module, it should be able to increase to 16 GB capacity.	<i>Teklif edilen ürünün sistem belleği en az 2 GB DDR3 olmalıdır. Bellek modülü ilavesi ile 16 GB kapasiteye çıkabilmelidir.</i>
6.7.	The proposed processor architecture must be at least 64 bits, at least four	<i>Teklif edilen işlemci mimarisi en az 64 bit, en az dört çekirdek en az 2.4 GHz olmalıdır.</i>

	cores must be at least 2.4 GHz.	
6.8.	The proposed product must support 2.5" and 3.5" SATA and SSD discs.	<i>Teklif edilen ürün 2,5" ve 3,5" SATA ve SSD diskleri desteklemelidir.</i>
6.9.	The proposed product must have at least 2 USB 3.0, at least 1 eSATA, and at least 4 Gigabit Ethernet ports supporting Link Aggregation and Failover.	<i>Teklif edilen ürün üzerinde en az 2 adet USB 3.0, en az 1 adet eSATA ve en az 4 adet Link Aggregation ve Failover destekleyen 1 Gigabit Ethernet portu bulunmalıdır.</i>
6.10.	The proposed product must have at least 1 PCIe Expansion slot.	<i>Teklif edilen ürünün en az 1 adet PCIe Genişletme slotu bulunmalıdır.</i>
6.11.	The product to be offered will have a power adapter with a power of at least 250W.	<i>Teklif edilecek olan ürünün en 250W gücünde güç adaptörü bulunacaktır.</i>
6.12.	The device must be able to operate at temperatures from at least 5 °C to a maximum of 35 °C.	<i>Cihaz en az 5 °C ile en fazla 35 °C arasındaki sıcaklıklarda çalışabilmelidir.</i>
6.13.	The warranty period of the device must be at least 3 years.	<i>Cihazın garanti süresi en az 3 yıl olmalıdır.</i>
6.14.	The proposed product must support at least 512 folder shares.	<i>Teklif edilen ürün En az 512 adede kadar klasör paylaşımını desteklemelidir.</i>
6.15.	The number of products iSCSI targets on offer must be at least 128 pieces.	<i>Teklif edilen ürün iSCSI hedef sayısı en az 128 adet olmalıdır.</i>
6.16.	The number of iSCSI luns on offer must be at least 256 pieces.	<i>Teklif edilen ürün iSCSI lun sayısı en az 256 adet olmalıdır.</i>
6.17.	The proposed product must support CIFS, AFP, NFS, FTP, WebDAV file protocols.	<i>Teklif edilen ürün CIFS,AFP,NFS,FTP,WebDAV dosya protokollerini desteklemelidir.</i>
6.18.	The proposed product must support RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 builds.	<i>Teklif edilen ürün RAID 0, RAID 1, RAID 5, RAID 6 ve RAID 10 yapılarını desteklemelidir.</i>
6.19.	The proposed product must support at least 2048 local user accounts.	<i>Teklif edilen ürün en az 2048 adet yerel kullanıcı hesabını desteklemelidir.</i>
6.20.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	<i>Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
7. Network Switch Type 1 // <i>Ağ Anahtarı Tip 1</i>		1 piece // <i>1 adet</i>
Technical Specifications		
7.1.	At least 4 1/10 GbE SFP/SFP+ slots must be supported in the maximum configuration on the proposed switch.	<i>Teklif edilen anahtar üzerinde maksimum konfigürasyonda en az 4 adet 1/10 GbE SFP/SFP+ yuva desteklenebilmelidir.</i>
7.2.	At least 4 10G SR SFP+ Modules of the same brand as the manufacturer should be given with the proposed	<i>Teklif edilen anahtar ile üretici ile aynı marka en az 4 adet 10G SR SFP+ Modül verilmelidir.</i>

	switch.	
7.3.	The "Switching" capacity of the proposed switch must be at least 180 Gbps.	<i>Teklif edilen anahtarın "Switching" kapasitesi en az 180 Gbps olmalıdır.</i>
7.4.	The "Forwarding" capacity of the proposed switch must be at least 130 million packets per second (Mpps).	<i>Teklif edilen anahtarın "Forwarding" kapasitesi en az 130 million packet per second (Mpps) olmalıdır.</i>
7.5.	The proposed switch must have at least 48 Copper ports supporting the PoE+ standard at 10/100/1000.	<i>Teklif edilen anahtar üzerinde en az 48 adet 10/100/1000 hızında PoE+ standartını destekleyen Bakır port bulunmalıdır.</i>
7.6.	The POE power budget of the proposed switch must be at least 370W.	<i>Teklif edilen anahtarın POE güç bütçesi en az 370W olmalıdır.</i>
7.7.	The proposed switch must have 1 10/100 Mbps RJ-45 Ethernet Out of Band management port.	<i>Teklif edilen anahtar üzerinde 1 adet 10/100 Mbps RJ-45 Ethernet Out of Band management portu bulunmalıdır.</i>
7.8.	The proposed switch must be in the stackable architecture. At least 8 devices must be supported in a stack.	<i>Teklif edilen anahtar yığılanabilir mimaride olmalıdır. Bir yığın içerisinde en az 8 adet cihaz desteklenmelidir.</i>
7.9.	The stacking bandwidth of the proposed switch must be at least 40 Gbps.	<i>Teklif edilen anahtarın yığınlama bant genişliği en az 40 Gbps olmalıdır.</i>
7.10.	The proposed switch must be supplied with stacking modules if the cable required for stacking is required.	<i>Teklif edilen anahtar yığınlama için gerekli olan kablo gerekli ise yığınlama modülleri ile verilmelidir.</i>
7.11.	The unit must be insertable and removable while the stack is running. For this purpose, at least one of the "Online Insertion/Removal" or "Hot Insertion/Removal" features should be supported.	<i>Yığın çalışır durumdayken ünite eklenebilir ve çıkarılabilir özellikte olmalıdır. Bu amaçla "Online Insertion/Removal" veya "Hot Insertion/Removal" özelliklerinden en az birisi desteklenmelidir.</i>
7.12.	There must be at least 16,000 (sixteen thousand) MAC address support in the address table.	<i>Adres tablosunda en az 16.000 (onaltıbin) adet MAC adresi desteği olmalıdır.</i>
7.13.	"MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" and "Per Vlan Rapid Spanning Tree + (PVST+)" must be supported on the proposed switch.	<i>Teklif edilen anahtar üzerinde "MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" ve "Per Vlan Rapid Spanning Tree + (PVST+)" desteklenmelidir.</i>
7.14.	120 ports (Etherchannel/Link Aggregation Group/Trunk Group/Multi Trunk Link) must be created using the IEEE 802.3ad Link Aggregation protocol feature. At least 8 ports must be members of a "Link Aggregation Group".	<i>IEEE 802.3ad Link Aggregation protokolü özelliğini kullanarak 120 adet bağlantı noktası (Etherchannel/Link Aggregation Group/Trunk Group/Multi Link Trunk) oluşturulabilmelidir. Bir "Link Aggregation Group" 'a en az 8 adet port üye olabilmelidir.</i>
7.15.	At least 4000 (four thousand) VLAN configurations must be supported in	<i>IEEE 802.1Q standardında en az 4000 (dört bin) adet VLAN konfigürasyonu</i>

	the IEEE 802.1Q standard.	<i>desteklenmelidir.</i>
7.16.	At least one of the "RFC 3176 sFlow" or "Netflow" protocols must be supported in order to perform traffic analysis.	<i>Trafik analizi yapabilmek için "RFC 3176 sFlow" veya "Netflow" protokollerinden en az biri desteklenmelidir.</i>
7.17.	Static routing, RIPv1/v2, and RIPv6 must be supported for IPv4 and IPv6 protocols.	<i>IPv4 ve IPv6 protokolleri için statik yönlendirme, RIPv1/v2 ve RIPv6 desteklenmelidir.</i>
7.18.	OSPF v2/v3 dynamic routing protocols must be supported by obtaining a license or software update on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile OSPF v2/v3 dinamik yönlendirme protokolleri desteklenebilir.</i>
7.19.	At least 1000 (thousand) directional registrations must be supported.	<i>En az 1000 (bin) adet yön kaydı desteklenmelidir.</i>
7.20.	The "VRRP-E" or "HSRP" gateway must support at least one of the backup protocols by obtaining a license or software update on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile "VRRP-E" veya "HSRP" ağ geçidi yedekleme protokollerinden en az birini desteklemelidir.</i>
7.21.	MLD snooping v1, v2 must be enabled so that IPv6 multicast traffic can be routed to the necessary interfaces and unnecessary multicast broadcasting can be blocked.	<i>IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping v1, v2 özelliği bulunmalıdır.</i>
7.22.	PIM-SM (PIM Sparse Mode) and PIM-SSM (Source Specific Multicast) must be supported from dynamic multicast routing protocols with license or software updates on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile dinamik multicast yönlendirme protokollerinden PIM-SM (PIM Sparse Mode) ve PIM-SSM (Source Specific Multicast) desteklenmelidir.</i>
7.23.	RADIUS and TACACS protocols and identification features should be supported.	<i>RADIUS ve TACACS protokolleri ile kimlik tanımlama özelliklerini desteklenmelidir.</i>
7.24.	Access checklists must be supported.	<i>Erişim kontrol listeleri desteklenmelidir.</i>
7.25.	At least one of the "Broadcast, multicast and unknown unicast rate-limiting" or "Storm Control" features must be supported.	<i>"Broadcast, multicast and unknown unicast rate limiting" veya "Storm Control" özelliklerinden en az birisi desteklenmelidir.</i>
7.26.	DHCP Relay, DHCP Server, and DHCP snooping features must be supported.	<i>DHCP Relay, DHCP Server ve DHCP snooping özelliklerini desteklenmelidir.</i>
7.27.	The "Dynamic ARP Inspection" feature should be supported to protect against network attacks.	<i>Ağ ataklarına karşı koruma amaçlı "Dynamic ARP Inspection" özelliği desteklenmelidir.</i>
7.28.	The "BPDU guard" feature must be supported to protect the "Spanning Tree" structure against external attacks.	<i>"Spanning Tree" yapısını dış ataklara karşı korumak için "BPDU guard" özelliği desteklenmelidir.</i>
7.29.	The "Root Guard" feature must be supported to protect the selected	<i>"Spanning Tree Root" seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı</i>

	switch from attacks and configuration errors.	<i>korumak için "Root Guard" özelliği desteklenmelidir.</i>
7.30.	At least one of the "Multi-Device Authentication" or "Multidomain Authentication" features must be supported to support more than one 802.1x user per port at the same time.	<i>Port başına aynı anda birden fazla 802.1x kullanıcısının desteklenebilmesi adına "Multi Device Authentication" veya "Multidomain Authentication" özelliklerinden en az birisi desteklenmelidir.</i>
7.31.	"VLAN Based Mirroring" or "VLAN ACL (VACL)" must be supported.	<i>"VLAN Based Mirroring" veya "VLAN ACL (VACL)" desteklenmelidir.</i>
7.32.	Support for "Uni-Directional Link Detection (UDLD)" should be available to protect the health of connections between switching devices.	<i>Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı "Uni-Directional Link Detection (UDLD)" desteği bulunmalıdır.</i>
7.33.	Cisco Discovery Protocol (CDP) or LLDP protocol must be supported to learn about neighboring devices.	<i>Komşu cihazları öğrenebilmek amacıyla Cisco Discovery Protocol (CDP) ya da LLDP protokolünü desteklenmelidir.</i>
7.34.	Support for the "IEEE 802.1AB LLDP-MED" protocol must be available for automatic settings of edge devices such as IP Phones, such as QoS and VLAN.	<i>IP Telefon gibi uç cihazların QoS ve VLAN gibi ayarlarının otomatik olarak yapılabilmesi için "IEEE 802.1AB LLDP-MED" protokolü desteği bulunmalıdır.</i>
7.35.	It must have support for marking the values "IEEE 802.1p" and "DSCP".	<i>"IEEE 802.1p" ve "DSCP" değerlerini işaretleme (marking/remarking) desteğine sahip olmalıdır.</i>
7.36.	At least 8 priority/output queues (Priority/Egress Queue) must be defined.	<i>En az 8 adet öncelik/çıkış kuyruğu (Priority/Egress Queue) tanımlanabilmelidir.</i>
7.37.	There must be support for applying speed restriction to traffic determined according to the access control list.	<i>Erişim kontrol listesine göre belirlenmiş bir trafiğe hız sınırlama uygulama desteği olmalıdır.</i>
7.38.	The "SCP Secure Copy" protocol must be supported for secure file transfer purposes.	<i>Güvenli dosya transferi amacıyla "SCP Secure Copy" protokolü desteklenmelidir.</i>
7.39.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	<i>Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
8. Network Switch Type 2 (NON-POE) // <i>Ağ Anahtarı Tip 2 (POE Olmayan)</i>		2 pieces // <i>2 adet</i>
Technical Specifications		
8.1.	At least 4 1/10 GbE SFP/SFP+ slots must be supported in the maximum configuration on the proposed switch.	<i>Teklif edilen anahtar üzerinde maksimum konfigürasyonda en az 4 adet 1/10 GbE SFP/SFP+ yuva desteklenebilmelidir.</i>
8.2.	The "Switching" capacity of the proposed switch must be at least 180	<i>Teklif edilen anahtarın "Switching" kapasitesi en az 180 Gbps olmalıdır.</i>

	Gbps.	
8.3.	The "Forwarding" capacity of the proposed switch must be at least 130 million packets per second (Mpps).	<i>Teklif edilen anahtarın "Forwarding" kapasitesi en az 130 million packet per second (Mpps) olmalıdır.</i>
8.4.	There must be at least 48 10/100/1000 RJ45 Copper ports on the proposed key.	<i>Teklif edilen anahtar üzerinde en az 48 adet 10/100/1000 RJ45 Bakır port bulunmalıdır.</i>
8.5.	The proposed switch must have 1 10/100 Mbps RJ-45 Ethernet Out of Band management port.	<i>Teklif edilen anahtar üzerinde 1 adet 10/100 Mbps RJ-45 Ethernet Out of Band management portu bulunmalıdır.</i>
8.6.	The proposed switch must be in the stackable architecture. At least 8 devices must be supported in a stack.	<i>Teklif edilen anahtar yığılanabilir mimaride olmalıdır. Bir yığın içerisinde en az 8 adet cihaz desteklenmelidir.</i>
8.7.	The stacking bandwidth of the proposed switch must be at least 40 Gbps.	<i>Teklif edilen anahtarın yığınlama bant genişliği en az 40 Gbps olmalıdır.</i>
8.8.	If the cable required for the proposed switch stacking is required, it must be supplied with stacking modules.	<i>Teklif edilen anahtar yığınlama için gerekli olan kablo gerekli ise yığınlama modülleri ile verilmelidir.</i>
8.9.	The unit must be insertable and removable while the stack is running. For this purpose, at least one of the "Online Insertion/Removal" or "Hot Insertion/Removal" features should be supported.	<i>Yığın çalışır durumdayken ünite eklenebilir ve çıkarılabilir özellikte olmalıdır. Bu amaçla "Online Insertion/Removal" veya "Hot Insertion/Removal" özelliklerinden en az birisi desteklenmelidir.</i>
8.10.	There must be at least 16,000 (hexadecimal) MAC address support in the address table.	<i>Adres tablosunda en az 16.000 (onaltıbin) adet MAC adresi desteği olmalıdır.</i>
8.11.	"MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" and "Per Vlan Rapid Spanning Tree + (PVST+)" must be supported on the proposed switch.	<i>Teklif edilen anahtar üzerinde "MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" ve "Per Vlan Rapid Spanning Tree + (PVST+)" desteklenmelidir.</i>
8.12.	120 ports (Etherchannel/Link Aggregation Group/Trunk Group/Multi Trunk Link) must be created using the IEEE 802.3ad Link Aggregation protocol feature. At least 8 ports must be members of a "Link Aggregation Group".	<i>IEEE 802.3ad Link Aggregation protokolü özelliğini kullanarak 120 adet bağlantı noktası (Etherchannel/Link Aggregation Group/Trunk Group/Multi Link Trunk) oluşturulabilmelidir. Bir "Link Aggregation Group" 'a en az 8 adet port üye olabilmelidir.</i>
8.13.	At least 4000 (four thousand) VLAN configurations must be supported in the IEEE 802.1Q standard.	<i>IEEE 802.1Q standardında en az 4000 (dört bin) adet VLAN konfigürasyonu desteklenmelidir.</i>
8.14.	At least one of the "RFC 3176 sFlow" or "Netflow" protocols must be supported in order to perform traffic analysis.	<i>Trafik analizi yapabilmek için "RFC 3176 sFlow" veya "Netflow" protokollerinden en az biri desteklenmelidir.</i>

8.15.	Static routing, RIPv1/v2, and RIPv6 must be supported for IPv4 and IPv6 protocols.	IPv4 ve IPv6 protokolleri için statik yönlendirme, RIPv1/v2 ve RIPv6 desteklenmelidir.
8.16.	OSPF v2/v3 dynamic routing protocols must be supported by obtaining a license or software update on request.	İstendiğinde lisans alınarak veya yazılım güncellemesi ile OSPF v2/v3 dinamik yönlendirme protokolleri desteklenebilir.
8.17.	At least 1000 (thousand) directional registrations must be supported.	En az 1000 (bin) adet yön kaydı desteklenmelidir.
8.18.	The "VRRP-E" or "HSRP" gateway must support at least one of the backup protocols by obtaining a license or updating software on request.	İstendiğinde lisans alınarak veya yazılım güncellemesi ile "VRRP-E" veya "HSRP" ağ geçidi yedekleme protokollerinden en az birini desteklemelidir.
8.19.	PIM-SM (PIM Sparse Mode) and PIM-SSM (Source Specific Multicast) must be supported from dynamic multicast routing protocols with license or software update on request.	İstendiğinde lisans alınarak veya yazılım güncellemesi ile dinamik multicast yönlendirme protokollerinden PIM-SM (PIM Sparse Mode) ve PIM-SSM (Source Specific Multicast) desteklenmelidir.
8.20.	MLD snooping v1, v2 must be enabled so that IPv6 multicast traffic can be routed to the necessary interfaces and unnecessary multicast broadcasting can be blocked.	IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping v1, v2 özelliği bulunmalıdır.
8.21.	RADIUS and TACACS protocols and identification features should be supported.	RADIUS ve TACACS protokolleri ile kimlik tanımlama özelliklerini desteklenmelidir.
8.22.	Access checklists must be supported.	Erişim kontrol listeleri desteklenmelidir.
8.23.	At least one of the "Broadcast, multicast and unknown unicast rate limiting" or "Storm Control" features must be supported.	"Broadcast, multicast and unknown unicast rate limiting" veya "Storm Control" özelliklerinden en az birisi desteklenmelidir.
8.24.	DHCP Relay, DHCP Server, and DHCP snooping features must be supported.	DHCP Relay, DHCP Server ve DHCP snooping özelliklerini desteklenmelidir.
8.25.	The "Dynamic ARP Inspection" feature should be supported to protect against network attacks.	Ağ ataklarına karşı koruma amaçlı "Dynamic ARP Inspection" özelliği desteklenmelidir.
8.26.	The "BPDU guard" feature must be supported to protect the "Spanning Tree" structure against external attacks.	"Spanning Tree" yapısını dış ataklara karşı korumak için "BPDU guard" özelliği desteklenmelidir.
8.27.	The "Root Guard" feature must be supported to protect the selected key from attacks and configuration errors.	"Spanning Tree Root" seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı korumak için "Root Guard" özelliği desteklenmelidir.
8.28.	At least one of the "Multi Device Authentication" or "Multidomain Authentication" features must be	Port başına aynı anda birden fazla 802.1x kullanıcısının desteklenebilmesi adına "Multi Device Authentication" veya "Multidomain

	supported to support more than one 802.1x user per port at the same time.	<i>Authentication" özelliklerinden en az birisi desteklenmelidir.</i>
8.29.	"VLAN Based Mirroring" or "VLAN ACL (VACL)" must be supported.	<i>"VLAN Based Mirroring" veya "VLAN ACL (VACL)" desteklenmelidir.</i>
8.30.	Support for "Uni-Directional Link Detection (UDLD)" should be available to protect the health of connections between switching devices.	<i>Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı "Uni-Directional Link Detection (UDLD)" desteği bulunmalıdır.</i>
8.31.	Cisco Discovery Protocol (CDP) must support CDP or LLDP protocol in order to learn about neighboring devices.	<i>Komşu cihazları öğrenebilmek amacıyla Cisco Discovery Protocol (CDP) ya da LLDP protokolünü desteklemelidir.</i>
8.32.	Support for the "IEEE 802.1AB LLDP-MED" protocol must be available for automatic settings of edge devices such as IP Phones, such as QoS and VLAN.	<i>IP Telefon gibi uç cihazların QoS ve VLAN gibi ayarlarının otomatik olarak yapılabilmesi için "IEEE 802.1AB LLDP-MED" protokolü desteği bulunmalıdır.</i>
8.33.	Must have support for marking the values "IEEE 802.1p" and "DSCP".	<i>"IEEE 802.1p" ve "DSCP" değerlerini işaretleme (marking/remarking) desteğine sahip olmalıdır.</i>
8.34.	At least 8 priority/output queues (Priority/Egress Queue) must be defined.	<i>En az 8 adet öncelik/çıkış kuyruğu (Priority/Egress Queue) tanımlanabilmelidir.</i>
8.35.	There must be support for applying speed restriction to traffic determined according to the access control list.	<i>Erişim kontrol listesine göre belirlenmiş bir trafiğe hız sınırlama uygulama desteği olmalıdır.</i>
8.36.	The "SCP Secure Copy" protocol must be supported for secure file transfer purposes.	<i>Güvenli dosya transferi amacıyla "SCP Secure Copy" protokolü desteklenmelidir.</i>
8.37.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	<i>Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
9. Wireless Access Point // <i>Kablosuz Erişim Noktası</i>		7 pieces // <i>7 adet</i>
Technical Specifications		
9.1.	It should be able to operate simultaneously in 2.4 GHz and 5 GHz Frequency bands.	<i>2.4 GHz ve 5 GHz Frekans bantlarında aynı anda çalışabilmelidir.</i>
9.2.	12.2. IEEE must support 802.11b/g/a/n/ac wave 2 standards.	<i>IEEE 802.11b/g/a/n/ac wave 2 standartlarını desteklemelidir.</i>
9.3.	12.3. 802.11n technology should support 20 MHz, and 40 Mhz signals in both 2.4 GHz and 5 GHz bands. 80 MHz signal should support 5 GHz signal in 802.11ac technology.	<i>802.11n teknolojisinde hem 2.4 GHz hem de 5 GHz bantlarında 20 MHz, ve 40 Mhz sinyalleri desteklemelidir. 802.11ac teknolojisinde 5 GHz bandında 80 MHz sinyali desteklemelidir.</i>

9.4.	12.4. The following performance values must be supported: a) 802.11ac: 6.5 Mbps – 867 Mbps b) 802.11n: 6.5Mbps – 300 Mbps c) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps d) 802.11b: 11, 5.5, 2, 1 Mbps	<i>Aşağıdaki performans değerleri desteklenmelidir: a) 802.11ac: 6.5 Mbps – 867 Mbps b) 802.11n: 6.5Mbps – 300 Mbps c) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps d) 802.11b: 11, 5.5, 2, 1 Mbps</i>
9.5.	Support Transmit BeamForming technology.	<i>Transmit BeamForming teknolojisini desteklemelidir.</i>
9.6.	It must have intelligent antenna technology that can dynamically shape the broadcast area and provide advanced RF management by changing antenna coverage. 128 different broadcast areas must be dynamically created. In this way, an additional gain of 4 dB should be achieved in the direction of Transmit to antenna power. Thanks to the dynamically shaped broadcast area, signals should not be sent in directions where there is no communication, such broadcasts should be weakened at a rate of 10 dB.	<i>Dinamik olarak yayın alanını şekillendirebilen akıllı bir anten teknolojisine sahip olmalı ve anten kapsama alanlarını değiştirerek ileri düzey RF yönetimi sağlamalıdır. 128 farklı yayın alanı dinamik olarak yaratılabilmelidir. Bu sayede anten gücüne Transmit yönünde 4 dB ilave kazanç sağlanabilmelidir. Dinamik olarak şekillendirilebilen yayın alanı sayesinde haberleşmenin olmadığı yönlerde sinyal gönderilmemeli, bu tür yayınlar 10 dB oranında zayıflatılmalıdır.</i>
9.7.	Radio Frequency output power should be 23 dBm for 2.4 GHz and 23 dBm for 5 GHz.	<i>Radio Frekansı çıkış gücü 2.4 GHz için 23 dBm, 5 GHz için 23 dBm olmalıdır.</i>
9.8.	Reception sensitivity must be up to -101 dBm.	<i>Alış hassasiyeti -101 dBm'e kadar olmalıdır.</i>
9.9.	Must have at least 2x2 MIMO antenna structure.	<i>En az 2x2 MIMO anten yapısına sahip olmalıdır.</i>
9.10.	At least 2 Spatial-Streams must be supported.	<i>En az 2 Spatial-Stream desteklenmelidir.</i>
9.11.	Support 256 users at the same time.	<i>Aynı anda 256 kullanıcı desteklemelidir.</i>
9.12.	The channel must be able to select automatically.	<i>Kanal seçimini otomatik yapabilmelidir.</i>
9.13.	Background Scanning should allow you to detect interference (interference) in high-density environments and automatically select the appropriate channel by avoiding them.	<i>Background Scanning yaparak yüksek yoğunluklu ortamlardaki girişimleri (paraziti) tespit edebilme ve bunlardan sakınarak uygun kanalı otomatik olarak seçme özelliği bulunmalıdır.</i>
9.14.	IP multicast video stream support must be available.	<i>IP multicast video stream desteği bulunmalıdır.</i>
9.15.	IPv6 support must be available.	<i>IPv6 desteği bulunmalıdır.</i>
9.16.	The device should be able to analyze packages automatically and assign them to the relevant queues using	<i>Cihaz paketleri otomatik olarak analiz edebilmeli, gecikmeye duyarlı trafik için ileri düzey servis kalitesi, paket sınıflandırma ve</i>

	advanced service quality, packet classification, and automatic prioritization for latency-sensitive traffic.	<i>otomatik öncelik belirleme özelliklerini kullanarak bunları ilgili kuyruklara atayabilmelidir.</i>
9.17.	There should be fair airtime fairness support.	<i>Adil yayın zamanı kullanım desteği (Airtime Fairness) olmalıdır.</i>
9.18.	It should have the ability to automatically detect the highest performance channel and adjust itself to it. It should not interrupt communication with computers when scanning all channels for the purpose of detecting the highest performance channel.	<i>En yüksek performanslı kanalı otomatik olarak tespit edip kendisini o kanala ayarlama özelliği olmalıdır. En yüksek performanslı kanalı tespit amacıyla tüm kanalları tararken bilgisayarlarla olan iletişimi kesmemelidir.</i>
9.19.	It should have VLAN support.	<i>VLAN desteği olmalıdır.</i>
9.20.	WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i must support security features.	<i>WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i güvenlik özelliklerini desteklemelidir.</i>
9.21.	Support port-based 802.1x security features over RADIUS (both authenticator and supplicant).	<i>Port tabanlı 802.1x güvenlik özelliklerini RADIUS üzerinden desteklemelidir (hem authenticator hem de supplicant olarak).</i>
9.22.	It should have BandSteering capability and be able to force both 2.4 GHz and 5 GHz supported computers to connect over 5 GHz for load sharing when necessary.	<i>BandSteering özelliği olmalı ve gerekli görüldüğünde yük paylaşımı için hem 2.4 GHz hem de 5 GHz destekli bilgisayarları öncelikle 5 GHz üzerinden bağlanmaya zorlayabilmelidir.</i>
9.23.	16 BSSIDs should be supported where security and service quality policies can be set separately.	<i>Güvenlik ve servis kalitesi politikalarının ayrı ayrı ayarlanabileceği 16 adet BSSID desteklenmelidir.</i>
9.24.	Support router feature including NAT and DHCP services.	<i>NAT ve DHCP servislerini de içeren router özelliğini desteklemelidir.</i>
9.25.	HotSpot WLAN must dynamically have a user-by-user speed restriction feature.	<i>HotSpot WLAN için dinamik olarak kullanıcı bazında hız kısıtlama özelliği olmalıdır.</i>
9.26.	It must be configured independently from the command line (Telnet/SSH), web interface (http/s), via Controller switch, via SNMP v1,2,3 software. Must support TR-069.	<i>Bağımsız olarak komut satırından (Telnet/SSH), Web ara-yüzünden (http/s), Controller switch üzerinden, SNMP v1,2,3 yazılımı üzerinden konfigürasyonu yapılabilmelidir. TR-069 desteği olmalıdır.</i>
9.27.	Be able to make software updates with FTP and TFTP.	<i>FTP ve TFTP ile yazılım güncellemeleri yapabilmelidir.</i>
9.28.	It must be able to operate independently or in a controller control.	<i>Bağımsız olarak veya bir controller denetiminde çalışabilmelidir.</i>
9.29.	When working independently, L2TP must be able to tunnel between it and the head office.	<i>Bağımsız olarak çalışırken merkez ofisle arasında L2TP tünel oluşturabilmelidir.</i>

9.30.	When used with the controller it must support the following features : a) Authentication must be performed through the local database on the controller, via Active Directory, LDAP, or RADIUS server. b) Access control and load sharing between AP devices. c) Captive Portal and Guest user accounts that can authenticate over the web should be supported. d) In order to be able to roam quickly in voip and 802.1x EAP related applications, a tunnel must be established between the controller and the AP.	<i>Controller ile birlikte kullanıldığında aşağıdaki özellikleri desteklemelidir :</i> i. <i>Kimlik doğrulama işlemleri controller üzerindeki yerel veri tabanı üzerinden, Active Directory, LDAP veya RADIUS server üzerinden yapabilmelidir.</i> ii. <i>Erişim kontrolü ve AP cihazları arasında yük paylaşımı olmalıdır.</i> iii. <i>Web üzerinden kimlik doğrulaması yapabilen Captive Portal ve Misafir kullanıcı hesapları desteklenmelidir.</i> iv. <i>VoIP ve 802.1x EAP ile ilgili uygulamalarda hızlı roaming yapabilmek için controller ile AP arasında tünel oluşturulabilmelidir.</i>
9.31.	Must have the following physical characteristics: a) Be able to feed on 12 VDC or PoE. If the DC adapter is received, it must be able to operate between 110-240 VAC. b) Power consumption should be no more than 13W. c) It should be able to operate between 0°C and +40°C. d) Be able to work in relative humidity environments up to 95%. e) Kensington lock against theft should be possible. f) It must have a locking mechanism that will prevent accidental exit/fall from where it is installed. g) There must be one 10/100/1000BaseT Gigabit Ethernet port on it and it must be able to receive electricity via PoE. This port auto MDX should support auto-sensing. h) PoE power requirement must be within 802.3af standards. i) Energy saving feature.	<i>Aşağıdaki fiziki özelliklere sahip olmalıdır:</i> a) <i>12 VDC ile veya PoE üzerinden beslenebilmelidir. DC adaptör alınmışsa 110-240 VAC arasında çalışabilmelidir.</i> b) <i>Güç tüketimi en fazla 13W olmalıdır.</i> c) <i>0°C ile +40°C arasında çalışabilmelidir.</i> d) <i>%95'e kadar bağıl nem ortamlarında çalışabilmelidir.</i> e) <i>Çalınmaya karşı Kensington kilit imkânı olmalıdır.</i> f) <i>Monte edildiği yerden kazara çıkmayı/düşmeyi engelleyecek bir kilit mekanizmasına sahip olmalıdır.</i> g) <i>Üzerinde bir adet 10/100/1000BaseT Gigabit Ethernet port olmalıdır ve bu port PoE üzerinden elektrik alabilmelidir. Bu port auto MDX, auto-sensing özelliğini desteklemelidir.</i> h) <i>PoE güç ihtiyacı 802.3af standartları</i>

		<i>İçinde olmalıdır.</i> <i>i) Enerji tasarruf özelliği olmalıdır.</i>
9.32.	Limited lifelong guarantee should be provided against manufacturing and labor defects.	<i>İmalat ve işçilik hatalarına karşı kısıtlı ömür boyu garanti sağlanmalıdır.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
10. Authentication and Network Access Control Software // <i>Kimlik Doğrulama ve Ağ Erişim Kontrol Yazılımı</i>		1 pieces // <i>1 adet</i>
Technical Specifications		
10.1.	The authentication and network access control platform can be offered to run on VMware infrastructure or as hardware.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, Vmware altyapısı üzerinde çalışacak şekilde veya donanım olarak teklif edilebilir.</i>
10.2.	The authentication and network access control platform must work in full compatibility with the proposed network switches and wireless access devices.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, teklif edilen ağ anahtarları ve kablosuz erişim cihazları ile tam uyumlu çalışmalıdır.</i>
10.3.	Authentication and network access control platform should not compromise system security, Vlan assignment, profiling, etc. In order to use its features, it should not request SNMP write right.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, sistem güvenliğini tehlikeye düşürmemeli, Vlan ataması, profilendirme vb. özelliklerin kullanılabilmesi amacıyla SNMP yazma (SNMP write) hakkı istememelidir.</i>
10.4.	Authentication and network access control platform should work using IEEE 802.1x protocol	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, IEEE 802.1x protokolünü kullanarak çalışmalıdır</i>
10.5.	The authentication and network access control platform should be able to work centrally. No additional hardware or software should be installed in the zones.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu merkezi olarak çalışabilmelidir. Bölgelere ayrıca donanım veya yazılım kurulması gerekmemelidir.</i>
10.6.	The authentication and network access control platform should be available for both wired and wireless network and VPN.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu hem kablolu hem kablosuz ağ hem de VPN için kullanılabilmelidir.</i>
10.7.	Authentication and network access control platform should work with RADIUS protocol.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu RADIUS protokolü ile çalışmalıdır.</i>
10.8.	Authentication and network access control platform should be managed through a single management screen.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu tek bir yönetim ekranı üzerinden yönetilmelidir.</i>

10.9.	Authentication and network access control platform for the network , including the last, which users / devices identity, group, device make and model, contact tour (wireless is) physically being connected location , post, applications running on running malicious software, if any, etc. must be able to see / learn information and take action accordingly.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu Ağa dahil olan son kullanıcı/cihazların kimlik, grup, cihaz marka ve modeli, bağlantı turu, (kablosuz ise) bağlandığı fiziksel lokasyon, postur, üzerinde çalışan uygulama, varsa üzerinde çalışan zararlı yazılımlar vs. bilgileri görebilmeli/öğrenebilmeli ve bunlara göre aksiyon alabilmelidir.</i>
10.10.	Authentication and network access control platform should be able to act as NAC, it should be able to determine the current status of the operating system and antivirus application on the client, USB connection, disk encryption, etc. should be able to control.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu NAC görevi yapabilmeli, istemci üzerindeki işletim sistemi ve anti virüs uygulamasının güncellik durumlarını, USB bağlantısını, disk kriptosunu vs. kontrol edebilmelidir.</i>
10.11.	The authentication and network access control platform must be licensed for at least 500 endpoints . The duration of the offered licenses must be at least 5 years.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu en az 500 endpoint için lisanslanmalıdır. Teklif edilen lisansların süresi en az 5 yıl olmalıdır.</i>
10.12.	The system to be proposed should be able to work with all network devices that are IEEE 802.1x compliant and independent of the brand.	<i>Teklif edilecek sistem, IEEE 802.1x uyumlu marka bağımsız tüm ağ cihazları ile çalışabilmelidir.</i>
10.13.	The system to be proposed should be able to authorize MAC for devices that do not support IEEE 802.1x .	<i>Teklif edilecek sistem, IEEE 802.1x desteği olmayan cihazlar için MAC yetkilendirmesi yapabilmelidir.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
11. Firewall // <i>Güvenlik Duvarı</i>		1 pieces // <i>1 adet</i>
Technical Specifications		
11.1.	The proposed system must have at least the following features as the next generation firewall features. • Firewall • IPSec VPN Termination System • SSL VPN Termination System • Intrusion Detection and Prevention System (IPS) • Application Recognition and	<i>Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari aşağıdaki özelliklerde olmalıdır.</i> • <i>Güvenlik Duvarı (Firewall)</i> • <i>IPSec VPN Sonlandırma Sistemi</i> • <i>SSL VPN Sonlandırma Sistemi</i> • <i>Saldırı Tespit ve Engelleme Sistemi (IPS)</i> • <i>Uygulama Tanıma ve Kontrolü</i>

	Control System • Virus / Malicious Content Control • URL Category Filtering • Bandwidth management	(Application Control) Sistemi • Virüs/Zararlı İçerik Kontrolü • URL Kategori Filtreleme • Bant genişliği yönetimi
11.2.	These features should be provided with a single device as a hardware solution of the manufacturer. However, in case IPSec VPN and SSL VPN features cannot be supported when positioned Transparent; It can be provided with the virtual firewall feature on the same system or with a separate hardware product from the same manufacturer.	<i>Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlanmalıdır. Fakat IPSec VPN ve SSL VPN özelliklerinin Transparan konumlandırıldığında desteklenememesi durumunda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.</i>
11.3.	The device can operate as a single physical firewall, and in any case, it must be configured to run at least 10 virtual firewalls if the organization needs it.	<i>Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, her halukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.</i>
11.4.	The proposed Network Firewall must support Active-Active and Active-Passive operation for High-Availability. It should be able to share load while Active-Active. In case of failure of one of the devices, the other device should be able to continue operating by undertaking all functions.	<i>Teklif edilen Ağ Güvenlik Duvarı, High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.</i>
11.5.	The system must have SPI (Stateful Packet Inspection) Firewall feature.	<i>Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.</i>
11.6.	The system will detect and block spoofed packets.	<i>Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır.</i>
11.7.	Each of the network interfaces in the system; It must be able to be defined as LAN, WAN, DMZ, or user-nameable segments. The system should support IEEE 802.1Q VLAN and defined VLANs should be used as an interface.	<i>Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilir.</i>
11.8.	When offered with System Virtual Firewall feature; Physical and virtual interfaces on the system should be able to be shared between Virtual Firewalls. Virtual Firewalls should be managed independently from each	<i>Sistem Sanal Güvenlik Duvarı özelliği ile teklif edildiği durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız</i>

	other in terms of rules and routing.	<i>olarak yönetilebilmelidir.</i>
11.9.	System; It must be able to work on Layer3 (routing mode) and Layer2 (transparent mode) layers. While the desired virtual firewall systems on the system can work in Layer3, the desired virtual firewalls must be able to work transparently on Layer2 at the same time.	<i>Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilmelidir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilmelidir.</i>
11.10.	It should provide the following features in Transparent mode: • SPI (stateful packet inspection), • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control on Gateway • URL Category Filtering	<i>Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır:</i> • <i>SPI (stateful packet inspection),</i> • <i>Saldırı Tespit ve Engelleme Sistemi (IPS)</i> • <i>Uygulama Tanıma ve Kontrolü (Application Control) Sistemi</i> • <i>Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü</i> • <i>URL Kategori Filtreleme</i>
11.11.	In routing mode, it should provide the following features: • SPI (stateful packet inspection), • IPSec VPN Termination, • SSL VPN Termination, • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control • URL Category Filtering • Bandwidth control • Static routing,	<i>Routing modda aşağıdaki özellikleri sağlamalıdır;</i> • <i>SPI (stateful packet inspection),</i> • <i>IPSec VPN Sonlandırma,</i> • <i>SSL VPN Sonlandırma,</i> • <i>Saldırı Tespit ve Engelleme Sistemi (IPS)</i> • <i>Uygulama Tanıma ve Kontrolü (Application Control) Sistemi</i> • <i>Virüs/Zararlı İçerik Kontrolü</i> • <i>URL Kategori Filtreleme</i> • <i>Bant genişliği kontrolü</i> • <i>Statik yönlendirme (static routing),</i> • <i>RIP, OSPF ve BGP yönlendirme</i>

	• RIP must support OSPF and BGP routing protocols. If a license or extra software is required to provide these routing protocols, it must have been provided. • Server load balancing • WIFI Access Point controller • WAN optimization	<i>protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır.</i> • <i>Sunucu yük dengeleme</i> • <i>WIFI Access Point kontrolcüsü</i> • <i>WAN optimizasyon</i>
11.12.	The Network Security System should support multiple Wide Area Network (WAN) connections, and be able to use more than one Internet connection as redundant.	<i>Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli olarak kullanabilmelidir.</i>
11.13.	Network Security System must support Policy Based Routing.	<i>Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.</i>
11.14.	The system must have DHCP Server and DHCP Relay feature.	<i>Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.</i>
11.15.	Firewall policies should be able to be written on the network interface and / or zone basis on the system .	<i>Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.</i>
11.16.	Firewall policies should be written on the basis of user and user groups. Must have AD integration for user information .	<i>Güvenlik duvarı politikaları, kullanıcı ve kullanıcı grupları bazında yazılabilmelidir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.</i>
11.17.	The system should be able to do rule-based traffic shaping and traffic prioritization for Bandwidth Control . The system must support QoS and Differentiated Services. • Traffic formatting should also be defined in rules written on the basis of source, destination, and protocol (such as SMTP, FTP, DNS, H323). • The maximum and / or guaranteed bandwidth value	<i>Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme, ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.</i> • <i>Kaynak, hedef, ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı da yapılabilmelidir.</i> • <i>Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.</i>

	should be defined by priority value (such as low, medium, high). • Bandwidth control on per-IP basis should be possible when required. In this way, it should be ensured that the bandwidth defined for each resource allowed on the same rule is guaranteed. • Contrary to Article above, it should be ensured that the bandwidth defined for each resource allowed within the same rule can be used in common. • It should be able to control bandwidth on the basis of application. • Bandwidth control should be possible in inbound and outbound direction for the same traffic. Thus, while bandwidth can be specified in the outbound line for a permitted connection, a different bandwidth should be applied for the traffic corresponding to this connection.	• <i>İstenildiğinde per-IP bazında bant genişliği kontrolü yapılabilir.</i> Bu sayede aynı kural üzerinden izin verilen her kaynak için tanımlanan bant genişliğinin garanti edilmesi sağlanmalıdır. • <i>Üstteki maddenin aksine tüm aynı kural dahilinde izin verilen her kaynak için tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilir.</i> • <i>Uygulama bazında bant genişliği kontrolü yapılabilir.</i> • <i>Aynı trafik ile ilgili Inbound ve outbound doğrultuda bant genişliği kontrolü yapılabilir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilir.</i>
11.18.	Security System; It must be able to authenticate and authorize over the user database defined on it, RADIUS	<i>Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme</i>

	and LDAP.	yapabilmelidir.
11.19.	The system must have application control feature. System; It should be able to recognize, control and block traffic of at least 3,000 (three thousand) applications, such as messaging (such as MSN, ICQ, Yahoo, AOL), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella, etc.) and Web Applications, regardless of the port used. Applications recognized within the scope of application control should be updated with an update service over the internet.	<i>Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.</i>
11.20.	It should be possible to control whether the policy-based firewall logs start / stop in sessions.	<i>Politika bazlı firewall'un oturumlarda start/stop loglayıp / loglamaması denetlenebilmelidir.</i>
11.21.	Firewall, NAT, and all layer7 security functions provided should be able to be enabled in granular form on a rule-based basis "only for traffic that meets the specified criteria".	<i>Firewall, NAT ve sunulan tüm layer7 güvenlik fonksiyonları granüler şekilde "sadece belirlenen kriterlere uyan trafik için" kural bazlı devreye alınabilmelidir.</i>
11.22.	Daily operation operations should be able to be performed to a large extent (without the need to operate on the CLI) via WebGUI. On the other hand, the entire configuration should be able to be intervened in bulk via CLI.	<i>WebGUI üzerinden günlük operasyon işlemleri büyük oranda (CLI üzerinde işlem yapmaya gerek olmadan) gerçekleştirilebilmelidir. CLI üzerinden ise tüm konfigürasyona bulk şekilde müdahale edilebilmelidir.</i>
11.23.	The application control policy should be set in each firewall rule written on the basis of source (IP and / or user), target, service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.</i>
11.24.	The system should support IPSec VPN as VPN Gateway. DES must support MD5 and SHA-1 with 3DES, AES Encryption. There should be support for IKE and PKI. IPSEC VPN functions should be able to perform at hardware level performance on special ASIC-architecture hardware without straining the main resources of the system.	<i>Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır. IPSEC VPN işlevleri ASIC mimarili özel hardware üzerinde sistem ana kaynaklarını yormadan donanımsal seviyede performanslı gerçekleştirilebilmelidir.</i>
11.25.	The IPS system should be able to detect and stop Traffic and Protocol anomalies , as well as recognize and stop signature-based attacks. IPS signatures should be able to be	<i>IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir.</i>

	updated automatically with the update service over the internet. The update process should also be able to be done manually.	<i>Güncelleme işlemi manuel olarak ta yapılabilmelidir.</i>
11.26.	It should allow system administrators to create and block weakness signatures specific to the organization / need .	<i>Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkan sağlamalıdır.</i>
11.27.	IPS policy should be set in every firewall rule written on the basis of source (IP and / or user), target, service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.</i>
11.28.	The proposed Network security system should be able to detect and block Botnet activity.	<i>Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.</i>
11.29.	By analyzing the behavior of user traffics, it should allow easy detection of user machines displaying abnormal behavior on the graphical interface. All behaviors between layer3-layer7, such as traffic blocked through the firewall, attempts to access inappropriate web categories, running risky applications, communication with botnet sites, should be determined by weighing determinable scoring. In this way, it is aimed to detect a zero-day activity whose signature has not yet been published.	<i>Kullanıcı trafiklerinin davranış analizini yaparak, anormal davranış gösteren kullanıcı makinelerinin grafiksel arayüzde kolayca tesbitine olanak sağlamalıdır. Firewall üzerinden bloklanan trafikler, uygunsuz web kategorilerine erişim denemeleri, riskli uygulamaların çalışıyor olması, botnet siteleri ile haberleşme gibi layer3-layer7 arası tüm davranışlar ağırlığı belirlenebilir puanlama ile belirlenebilmelidir. Bu sayede henüz imzası yayınlanmamış bir sıfır-gün aktivitesinin tesbit edilmesi amaçlanmaktadır</i>
11.30.	The Network Security System must have SSL VPN Gateway feature in order to provide secure access of Mobile Users to Institution resources. SSL VPN client must support at least Windows, Mac OS, Linux operating systems and IOS, Android based mobile devices.	<i>Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.</i>
11.31.	TCP and UDP-based traffic must be tunneled through SSL VPN Gateway.	<i>SSL VPN Gateway içerisinden TCP ve UDP tabanlı trafikler tünellenebilmelidir.</i>
11.32.	SSL VPN feature will be offered with unlimited user license.	<i>SSL VPN özelliği sınırsız kullanıcı lisansı ile teklif edilecektir.</i>
11.33.	Users accessing via SSL VPN should be able to authenticate and authorize over the user database defined on the System, RADIUS, LDAP, and define internal and external resources that can be accessed with this	<i>SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.</i>

	authorization.	
11.34.	For users or systems accessing with SSL VPN and IPSEC VPN; SPI (stateful packet inspection), Intrusion Detection and Prevention System (IPS), Application Recognition and Control (Application Control) System, Virus / Malicious Content Control and URL Category Filtering, QoS and Bandwidth management features must be applicable.	<i>SSL VPN ve IPSEC VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, QoS ve Bant Genişliği yönetimi özellikleri uygulanabilir olmalıdır.</i>
11.35.	Malware detection and blocking feature must be available on the Network Firewall System. System; It should be able to prevent malicious software by scanning HTTP, SMTP, FTP, and POP3, IM (ICQ, MSN, Yahoo Messenger), MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB traffic. The system scans within the aforementioned protocols; It should be able to detect and stop threats such as Worm, Trojan, Keylogger, Spy, Dialer. Virus Control should be able to be performed between all network segments on the Network Firewall System. The AntiVirus system should be able to automatically update virus signatures over the Internet.	<i>Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem; HTTP, SMTP, FTP ve POP3, IM (ICQ, MSN, Yahoo Messenger) , MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir</i>
11.36.	AV control policy should be set in every firewall rule written on the basis of source (IP and / or user), target, service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.</i>
11.37.	There should be URL Filtering feature on the Network Security System. In this way, Category -based URL Filtering should be able to. Different categories of URL filtering should be able to be applied to different users and user groups.	<i>Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.</i>
11.38.	Different URL filtering policies should be set for each firewall rule written on the basis of source (IP and / or user), target, and service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir.</i>
11.39.	At least 75 URL categories on the system and more than 250 million were categorized URL should	<i>Sistem üzerinde en az 75 adet URL kategorisi ve 250 milyondan fazla kategorize edilmiş URL bulunmalıdır.</i>

	contain.	
11.40.	There should be no user limit for the URL Filtering function of the system and should be offered with an unlimited user license.	<i>Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.</i>
11.41.	Apart from URL filtering categories, the addresses requested as wildcard, regex, or full URL should be defined under different profiles (such as *.gov.tr *). Access to these defined addresses should be blocked or allowed.	<i>URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilir.</i>
11.42.	URL filtering warning screens can be customized.	<i>URL filtreleme uyarı ekranları özelleştirilebilecektir.</i>
11.43.	All systems offered must have IPv6 support and support dual-stack feature, which allows the use of IPv4 and IPv6 protocols at the same time. At least under IPv6; IPv6 addressing, IPv6 static routing, IPv6 DNS, IPv6 security rules, IPv6 recording and reporting, and Ping6 must be supported. IPS, Application Control, and Web Filtering should be able to be applied to IPv6 traffic.	<i>Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir. IPv6 trafiğine IPS, Uygulama Denetimi ve Web Filtreleme yapılabilir.</i>
11.44.	System configuration should be able to be done by at least the following methods: • With serial connection, through the console port, • With Http and Https connection, via web interface or via the manufacturer's own Linux or Windows based management application • With SSH connection, via the command line	<i>Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilir:</i> • Seri bağlantı ile konsol port üzerinden, • Http ve Https bağlantı ile web arayüz üzerinden veya üreticinin kendisine ait Linux veya Windows tabanlı yönetim uygulaması üzerinden • SSH bağlantı ile komut satırı (command line) üzerinden
11.45.	Network Firewall The system must support SNMP and must support SNMPv3	<i>Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir</i>
11.46.	Network Firewall System operating system and software updates must be	<i>Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web arayüzü, TFTP</i>

	made via the Web interface, TFTP or FTP.	<i>veya FTP üzerinden yapılabilirdir.</i>
11.47.	Updates of systems running redundantly should be able to be made at least via web gui. Systems should be able to be automatically updated sequentially without disrupting traffic.	<i>Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilirdir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.</i>
11.48.	There should be no user limit for the system about the Firewall, VPN, IPS functions and should be offered with an unlimited user license. Licenses to perform Software / operating system updates for 3 years and IPS, Application Recognition and Control, AntiVirus, URL Category Filtering services and updates for at least 3 years of the Network Security System must be provided with the system.	<i>Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.</i>
11.49.	The recommended firewall system manufacturer must have one or more of its products, entered the "NSS Labs Network IPS" and "NSS Labs Next Generation Firewall" tests and should be in the recommended product category.	<i>Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, "NSS Labs Network IPS" ve "NSS Labs Next Generation Firewall" testlerine girmiş ve tavsiye edilen ürün kategorisinde olması gereklidir.</i>
11.50.	The Firewall System must have a geographic database. It should be able to cut the traffic from the specified country or countries by writing a rule on a country basis.	<i>Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.</i>
11.51.	The proposed security system will also have load balancing features. • It should be able to load balance all sessions based on HTTP, HTTPS, SSL for Layer 7, TCP and UDP for Layer 4, and IP protocol for Layer 3. • IPS, AV policies should be available for servers with load balancing. • For HTTP and HTTPS	<i>Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.</i> • <i>Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP , Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.</i> • <i>Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilirdir.</i> • <i>HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin</i>

	connections, the source IP address should be able to go to physical servers. • Must have SSL Offloading feature for SSL connections. • Traffic should be able to be distributed to the real servers of the institution by the following methods: • Source IP hash information • Round robin • By making a weight definition in the real server definitions against the possibility of the servers having different powers • The traffic is sent to the first of the active real servers and the load is sent to the next active server in case of inactivity. • Based on responses to ping packets • Depending on the session number information directed to the servers • During load sharing, it should be able to check server availability by tcp, http (eg checking http://190.1.128.1/test_page.h	<i>gitmesi sağlanabilmelidir.</i> • <i>SSL bağlantıları için SSL Offloading özelliği olmalıdır.</i> • <i>Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:</i> • <i>Kaynak Ip hash bilgisi</i> • <i>Round robin</i> • <i>Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak</i> • <i>Aktif durumda olan gerçek sunuculardan ilkinde trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderilmesi</i> • <i>Ping paketlerine verilen cevaplar esas alınması</i> • <i>Sunucular üzerine yönlendirilen session sayı bilgisine bağlı olarak</i> <i>Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://190.1.128.1/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.</i>
--	---	--

	tm), and ping.	
11.52.	It should be able to perform vulnerability scanning tests on specified systems.	Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.
11.53.	The proposed system can work as a wifi controller, so it can be used for the management of wireless access devices that can be used.	Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılacak kablosuz erişim cihazlarının yönetimi için kullanılabilir.
11.54.	Wan will have optimization features.	Wan optimizasyon özelliklerine sahip olacaktır.
11.55.	It should be able to optimize the protocol for Common Internet File System (CIFS), FTP, HTTP, MAPI, and TCP sessions.	Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.
11.56.	Must have web cache feature.	Web cache özelliği olmalıdır.
11.57.	It must support Web cache communication Protocol (WCCP).	Web cache communication Protocol (WCCP) desteği olmalıdır.
11.58.	Proposed security system should have at least 10/10/6 Gbps Firewall performance value for 1518/512/64 Byte IP packet size in the proposed configuration. These values should be stated in the documentation for the product offered and the manufacturer should have posted these values publicly on his website.	Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, 1518/512/64 Byte IP paket büyüklüğü için en az 10/10/6 Gbps Firewall performansı değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
11.59.	The system must support at least 700 thousand sessions at the same time and must have a performance of at least 35 thousand new sessions per second. These values should be specified in the product documentation offered. These values should be stated in the documentation for the product offered and the manufacturer should have published these values publicly on his website.	Sistem aynı anda en az 700bin oturumu desteklemeli ve saniyede en az 35 Bin yeni oturum açabilme performansına sahip olmalıdır. Bu değerler teklif edilen ürün belgelerinde belirtilmiş olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
11.60.	Firewall System must have at least 6.5 Gbps IPSec VPN throughput for AES128 + SHA-1 . These values should be stated in the documentation for the product offered and the manufacturer should have published these values publicly on his website.	Güvenlik Duvarı Sisteminin AES128 + SHA-1 için en az 6.5 Gbps IPSec VPN throughput değerine sahip olmalıdır. Bu değerler teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.
11.61.	The system must support 200 Site-to-Site and at least 500 IPSec VPN tunnels	Sistem Site-to-Site 200 adet ve Client-to-Site için en az 500 adet IPSec VPN tünel

	for Client-to-Site. The device must be able to work compatible with VPN Gateway devices that comply with the standards that support the aforementioned VPN protocols.	<i>desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir</i>
11.62.	The system must have a performance rating of 1.4 Gbps IPS throughput. This value should be stated in the documentation for the product offered, and the manufacturer should have posted these values publicly on his website.	<i>Sistem 1.4 Gbps IPS throughput performans değerine sahip olmalıdır. Bu değer teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.</i>
11.63.	There should be at least 5 10/100/1000 Base-T and 2 Management Port ports on the system.	<i>Sistem üzerinde En az 5 adet 10/100/1000 Base-T, 2 adet Management Port bağlantı noktası olmalıdır.</i>
11.64.	The system must be able to send records to the Syslog Servers, to the Registration / Reporting System that will be offered with the System, and to keep records.	<i>Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmeli kayıt tutabilmelidir.</i>
11.65.	Log and Hotspot software that fully complies with the Law No. 5651 should be offered with the system.	<i>Sistemle birlikte 5651 nolu kanunu tam karşılayan Log ve Hotspot yazılımı teklif edilmelidir.</i>
11.66.	The proposed system must have a software and hardware warranty of at least 3 years. Licenses to perform Software / Firmware updates for 3 years must be given with the system.	<i>Teklif edilen sistemin en az 3 yıl yazılım ve donanım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
12. Personal Computer // <i>Bilgisayar</i>		2 pieces // <i>2 adet</i>
Technical Specifications		
12.1.	The computer to be offered must be a corporate product. The warranty period should be extended with additional packages.	<i>Teklif edilecek bilgisayar kurumsal ürün olmalıdır. Garanti süresi ek paketler ile uzatılabilmelidir.</i>
12.2.	The frame size of the computer must be in MFF form.	<i>Bilgisayarın kasa tipi MFF formunda olmalıdır.</i>
12.3.	The processor of the computer should have a minimum 2.2 GHz base CPU speed.	<i>Bilgisayarın işlemcisi en az 2.2 GHz temel hızında olmalıdır.</i>
12.4.	The computer's RAM memory must be at least 4GB.	<i>Bilgisayarın RAM hafızası en az 4GB olmalıdır.</i>
12.5.	The disk capacity of the computer must be at least 500GB.	<i>Bilgisayarın disk kapasitesi en az 500GB olmalıdır.</i>

12.6.	The operating system of the computer must be Windows 10 Pro or equivalent.	<i>Bilgisayarın işletim sistemi Windows 10 Pro ya da eşdeğeri olmalıdır.</i>
12.7.	There should be at least 4 USB 3.1 ports and at least 2 USB 2.0 ports on the computer. At least 2 of the USB ports should be located on the front of the case.	<i>Bilgisayarın üzerinde en az 4 adet USB 3.1 portu ve en az 2 adet USB 2.0 portu bulunmalıdır. USB portlarının en az 2 tanesi kasanın ön tarafında konumlandırılmalıdır.</i>
12.8.	The computer must have at least 1 RJ-45 ethernet port.	<i>Bilgisayarın en az 1 adet RJ-45 ethernet portu bulunmalıdır.</i>
12.9.	There should be at least 1 HDMI 1.4 and at least 1 DisplayPort 1.2 port on the computer for Monitor connection.	<i>Bilgisayarın üzerinde Monitör bağlantısı için en az 1 adet HDMI 1.4 ve en az 1 adet DisplayPort 1.2 portu bulunmalıdır.</i>
12.10.	There should be headphone and microphone jacks on the computer.	<i>Bilgisayarın üzerinde kulaklık ve mikrofon girişleri bulunmalıdır.</i>
12.11.	DVD-RW must be on the computer.	<i>Bilgisayar üzerinde DVD-RW bulunmalıdır.</i>
12.12.	The computer must have at least 2 M.2 slots.	<i>Bilgisayarın en az 2 adet M.2 yuvası bulunmalıdır.</i>
12.13.	At least 23.8" monitor of the same brand should be provided with the computer.	<i>Bilgisayar ile birlikte aynı marka en az 23.8" monitör verilmelidir.</i>
12.14.	The monitor must support 1920 x 1080 60Hz resolution.	<i>Monitör 1920 x 1080 60Hz çözünürlüğü desteklemelidir.</i>
12.15.	The brightness of the monitor should be at least 250cd / m2.	<i>Monitör ün parlaklığı en az 250cd/m2 olmalıdır.</i>
12.16.	The response time of the monitor should be at most 6ms.	<i>Monitör ün tepkime süresi en çok 6ms olmalıdır.</i>
12.17.	The monitor should have a depth of 16.7 Million colors.	<i>Monitör 16.7 Milyon renk derinliğine sahip olmalıdır.</i>
12.18.	The monitor should be visible horizontally and vertically at an angle of at least 178 degrees.	<i>Monitör yatayda ve dikeyde en az 178 derecelik açıda görülebilmelidir.</i>
12.19.	The monitor should be height adjustable.	<i>Monitörün yüksekliği ayarlanabilir olmalıdır.</i>
12.20.	The monitor must have anti-glare properties.	<i>Monitör parlama önleyici özelliğe sahip olmalıdır.</i>
12.21.	The same brand of wireless keyboard and wireless mouse should be given with the computer.	<i>Bilgisayar ile birlikte aynı marka kablosuz klavye ve kablosuz Mouse verilmelidir.</i>
12.22.	The individual computer and monitor must have a warranty period of at least 3 years.	<i>Teklil edilen bilgisayar ve monitör en az 3 yıl garanti süresine sahip olmalıdır.</i>

Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
13. Data Center Security Software // <i>Veri Merkezi Güvenlik Yazılımı</i>		1 pieces // 1 adet
Technical Specifications		
13.1.	All components that make up the Data Center Security Software to be offered will be a single product from the same manufacturer. Even if it belongs to the same manufacturer, it will not be a solution created by combining different products.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımını oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.</i>
13.2.	The Data Center Security Software to be offered will be capable of managing the security policies of server systems in physical, virtual, and cloud environments from a single point.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı fiziksel, sanal ve bulut ortamdaki sunucu sistemlerin güvenlik politikalarını tek bir noktadan yönetebilecek özellikte olacaktır.</i>
13.3.	The Data Center Security Software to be offered should be offered to license 10 servers.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı 10 adet sunucuyu lisanslayacak şekilde teklif edilmelidir.</i>
13.4.	The Data Center Security Software to be offered will consist of Central Management System and Operating system agent applications.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi ve İşletim sistemi ajan uygulamalarından oluşacaktır.</i>
13.5.	The Data Center Security Software to be offered will be able to run on the following operating system platforms: - Windows Server 2016 (64-bit) - Windows Server 2012 or 2012 R2 (64-bit) — Full Server or Server Core - Windows Server 2008 R2 (64-bit) - Windows Server 2008 (32-bit and 64-bit) - Windows Server 2003 SP2 or higher (32-bit and 64-bit) - Windows 10 or 10 TH2 (32-bit and 64-bit) - Windows 8.1 (32-bit and 64-bit) - Windows 8 (32-bit and 64-bit) - Windows 7 (32-bit and 64-bit) - Windows XP (32-bit and 64-bit) - Hyper-V on Windows 2012 R2, 2012, 2008 R2, 8, and 8.1	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı aşağıdaki işletim sistemi platformlarında çalışabilecektir:</i> - Windows Server 2016 (64-bit) - Windows Server 2012 or 2012 R2 (64-bit) — Full Server ya da Server Core - Windows Server 2008 R2 (64-bit) - Windows Server 2008 (32-bit ve 64-bit) - Windows Server 2003 SP2 ya da daha yükseği (32-bit ve 64-bit) - Windows 10 or 10 TH2 (32-bit ve 64-bit) - Windows 8.1 (32-bit ve 64-bit) - Windows 8 (32-bit ve 64-bit) - Windows 7 (32-bit ve 64-bit) - Windows XP (32-bit ve 64-bit) - Hyper-V on Windows 2012 R2, 2012, 2008 R2, 8, ve 8.1 - Red Hat Enterprise Linux 7 (32-bit ve

	• Red Hat Enterprise Linux 7 (32-bit and 64-bit) • Red Hat Enterprise Linux 6 (32-bit and 64-bit) • Red Hat Enterprise Linux 5 (32-bit and 64-bit) • CentOS 7 (32-bit and 64-bit) • CentOS 6 (32-bit and 64-bit) • CentOS 5 (32-bit and 64-bit) • Oracle Linux 7 (32-bit and 64-bit) • Oracle Linux 6 (32-bit and 64-bit) • Oracle Linux 5 (32-bit and 64-bit) • SUSE Enterprise Linux 12 (64-bit) • SUSE Enterprise Linux 11 SP1, SP2, and SP3 (32-bit and 64-bit) • CloudLinux 7 (32-bit and 64-bit) • CloudLinux 6 (32-bit and 64-bit) • Debian 7 (64-bit) • Debian 8 (64-bit) • Ubuntu 16.04 LTS (64-bit) • Ubuntu 14.04 LTS (64-bit) • Solaris 11, 11.2, or 11.3 (64-bit, SPARC, or x86) • Solaris 10 Update 11 (64-bit, SPARC, or x86)	64-bit) • Red Hat Enterprise Linux 6 (32-bit ve 64-bit) • Red Hat Enterprise Linux 5 (32-bit ve 64-bit) • CentOS 7 (32-bit ve 64-bit) • CentOS 6 (32-bit ve 64-bit) • CentOS 5 (32-bit ve 64-bit) • Oracle Linux 7 (32-bit ve 64-bit) • Oracle Linux 6 (32-bit ve 64-bit) • Oracle Linux 5 (32-bit ve 64-bit) • SUSE Enterprise Linux 12 (64-bit) • SUSE Enterprise Linux 11 SP1, SP2, ve SP3 (32-bit and 64-bit) • CloudLinux 7 (32-bit ve 64-bit) • CloudLinux 6 (32-bit ve 64-bit) • Debian 7 (64-bit) • Debian 8 (64-bit) • Ubuntu 16.04 LTS (64-bit) • Ubuntu 14.04 LTS (64-bit) • Solaris 11, 11.2, or 11.3 (64-bit, SPARC, ya da x86) • Solaris 10 Update 11 (64-bit, SPARC, ya da x86)
13.6.	The Data Center Security Software to be offered should support working in a highly accessible architecture.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı yüksek erişilebilir mimaride çalışmayı desteklemelidir.</i>
13.7.	The Data Center Security Software Central Management System to be proposed must support working on the following operating systems: • Windows Server 2016 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit) • Red Hat Enterprise Linux 7 (64-bit)	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi aşağıdaki işletim sistemleri üzerinde çalışmayı desteklemelidir:</i> • Windows Server 2016 (64-Bit) • Windows Server 2012 (64-Bit) • Windows Server 2012 R2 (64-Bit) • Red Hat Enterprise Linux 7 (64-Bit)
13.8.	The Data Center Security Software to be proposed should support working with the following systems as the Central Management System database. • Oracle Database 12c, • Microsoft SQL Server 2016 • Microsoft SQL Server 2014,	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi veritabanı olarak aşağıdaki sistemler ile çalışmayı desteklemelidir.</i> <i>Oracle Database 12c,</i> <i>Microsoft SQL Server 2016</i> <i>Microsoft SQL Server 2014,</i> <i>Microsoft SQL Server 2012,</i>

	• Microsoft SQL Server 2012, • Postgre SQL 9.6 (Core Distribution & Amazon RDS) • Microsoft SQL RDS or Oracle RDS	<i>Postgre SQL 9.6 (Core Distribution & Amazon RDS)</i> <i>Microsoft SQL RDS ya da Oracle RDS</i>
13.9.	On the Data Center Security Software to be offered, there will be intrusion detection and prevention, firewall, malware prevention, website reliability, integrity monitoring, log inspection, and application control components, and all components related to these functions will be offered.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde saldırı tespit ve önleme, güvenlik duvarı, zararlı yazılım önleme, web sitesi güvenilirliği, bütünlük gözleme, kütük inceleme ve uygulama kontrolü bileşenleri bulunacak, bu işlevlerle ilgili tüm bileşenler teklif edilecektir.</i>
13.10.	The attack detection and prevention component to be found on the Data Center Security Software to be proposed will be in an architecture that can scan incoming and outgoing traffic and work with deep packet inspection (DPI).	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak saldırı tespit ve önleme bileşeni gelen ve giden trafiği tarayabilecek ve derin paket inceleme (DPI) çalışabilecek mimaride olacaktır.</i>
13.11.	Virtual Patch functionality on Windows systems will be supported by the intrusion detection and prevention module that will serve on the proposed Data Center Security Software . When necessary, modules provided at network level can be switched to "monitoring" mode.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde hizmet verecek olan saldırı tespit ve önleme modülü marifeti ile Windows sistemler üzerinde Sanal Yama işlevi desteklenecektir. Gerekliği durumlarda ağ seviyesinde sağlanan modüller "izleme" moduna alınabilecektir.</i>
13.12.	The Data Center Security Software to be offered will include the virtual patch (host based IPS) feature. With the virtual patch feature, network vulnerabilities on the servers can be detected, and they can be turned off manually or automatically, optionally.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı, sanal yama (host based IPS) özelliğini barındıracaktır. Sanal yama özelliği ile sunucular üzerinde bulunan ağ zafiyetleri tespit edilebilecek, isteğe bağlı olarak manuel veya otomatik olarak kapatılabilecektir.</i>
13.13.	The firewall component to be found on the Data Center Security Software to be proposed must be capable of preventing denial of service attacks (DoS) and discovery scans.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak olan güvenlik duvarı bileşeni hizmet dışı bırakma saldırılarını (DoS) ve keşif taramalarını engelleme yeteneğine sahip olmalıdır.</i>
13.14.	Integrity monitoring component to be found on the proposed Data Center Security Software will be able to monitor and report changes in critical operating system files, directories, registry keys, and values in real-time	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak bütünlük gözleme bileşeni kritik işletim sistemi dosyaları, dizinleri, kayıt defteri (registry) anahtar ve değerlerindeki değişiklikleri gerçek zamanlı izleyerek rapor edebilecek, alarm</i>

	and generate alarms.	üretebilecektir.
13.15.	The log analysis component to be found on the Data Center Security Software to be proposed will be able to monitor the log records and logs of the operating system and applications on the operating system it is running on, and report suspicious situations and generate alarms.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak kütük inceleme bileşeni çalıştığı işletim sistemi üzerindeki işletim sistemi ve uygulamalara ait günlük kayıtları ve kütükleri izleyerek şüpheli durumları rapor edebilecek, alarm üretebilecektir.</i>
13.16.	The Data Center Security Software to be offered will be able to access the manufacturer's Global Threat Intelligence service, and with this service, it will be able to make reputation inquiries for web pages, electronic mail resources, and files.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üreticinin Global Tehdit İstihbarat hizmetine erişebilecek, bu hizmet sayesinde web sayfaları, elektronik posta kaynakları ve dosyalar için saygınlık sorguları yapabilecektir.</i>
13.17.	The Data Center Security Software to be offered will support integration with the same manufacturer's Detailed Analysis System for Advanced Attacks . With this integration , they will be able to send suspicious files for analysis. It will also be able to block files and URLs found as a result of the analysis.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı, aynı üreticinin Gelişmiş Saldırıları İçin Detaylı Analiz Sistemi ile entegrasyonu destekleyecektir. Bu entegrasyon ile şüpheli gördüğü dosyaları analize gönderebilecektir. Ayrıca analiz sonucu bulunan dosya ve URL leri bloklayabilecektir.</i>
Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
14. User Security Solution // <i>Kullanıcı Güvenliği Çözümü</i>		1 pieces // <i>1 adet</i>
Technical Specifications		
14.1.	All components to be offered will belong to the same manufacturer.	<i>Teklif edilecek tüm bileşenler aynı üreticiye ait olacaktır.</i>
14.2.	The "User Security" solution to be offered will be offered for at least 15 end users.	<i>Teklif edilecek "Kullanıcı Güvenliği" çözümü en az 15 son kullanıcı için teklif edilecektir.</i>
14.3.	The Anti-malware Software to be offered must support the endpoint platforms listed below. • Windows 7 SP1 • Windows 8.1 • Windows 10 • Windows Server 2008R2 (64bit) • Windows Server 2012 (64bit) • Windows Server 2012R2 (64bit) • Windows Server 2016 (64bit)	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aşağıda listelenen uç nokta platformlarını desteklemelidir.</i> • Windows 7 SP1 • Windows 8.1 • Windows 10 • Windows Server 2008R2 (64bit) • Windows Server 2012 (64bit) • Windows Server 2012R2 (64bit)

	• Windows Server 2019 (64bit)	• Windows Server 2016 (64bit) • Windows Server 2019 (64bit)
14.4.	The Anti-malware to be offered should support the database platforms listed below. • Microsoft SQL Server 2008 Express SP2 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 Express SP1 • Microsoft SQL Server 2016 • Microsoft SQL Server 2016 SP1 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aşağıda listelenen veritabanı platformlarını desteklemektedir.</i> • Microsoft SQL Server 2008 Express SP2 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 Express SP1 • Microsoft SQL Server 2016 • Microsoft SQL Server 2016 SP1 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017
14.5.	The Anti-malware Management server to be offered must be accessed and managed through the Web interface.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim sunucusuna Web ara yüzünden erişilmeli ve yönetim sağlanabilmelidir.</i>
14.6.	The communication between the Malware Prevention Software management server to be offered and the agent software to run on the end user systems must be encrypted in the AES-256 encryption standard.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim sunucusu ile son kullanıcı sistemler üzerinde çalışacak ajan yazılımı arasındaki iletişim AES-256 şifreleme standardında şifreli olarak gerçekleştirilebilmelidir.</i>
14.7.	The anti-malware software to be offered must be able to fully protect the operating systems on which it works against viruses, trojans, worms, and spyware, and must be able to provide full protection against malicious codes spreading over the network.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde çalıştığı işletim sistemlerini virüs, truva atı, worm ve spyware lere karşı tam olarak koruyabilmeli ve network üzerinden yayılan zararlı kodlara karşıda tam koruma sağlayabilmelidir.</i>
14.8.	The Malware Prevention Software to be offered will monitor the suspicious file encryption activities of such malicious software on client systems in order to detect ransomware type malware and will be able to stop these encryption activities by quarantining or terminating them.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ransomware türünde zararlı yazılımları tespit etmek üzere, bu tip zararlı yazılımların istemci sistemler üzerindeki şüpheli dosya şifreleme faaliyetlerini izleyecek ve bu şifreleme faaliyetlerini karantinaya alarak ya da sonlandırarak durdurabilecektir.</i>

14.9.	The Malware Prevention Software to be offered will be able to work with predictive machine learning method and detect malicious software without the need for virus signatures.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı öngörüsöl makine öğrenme yöntemi ile çalışabilecek, virüs imzalarına ihtiyaç duymadan zararlı yazılımları tespit edebilecektir.</i>
14.10.	The Anti-malware Software to be offered should be able to provide kernel-level protection against rootkits.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı rootkitlere karşı kernel seviyesinde koruma sağlayabilmelidir.</i>
14.11.	The Malware Prevention Software to be offered should provide a website rating service that will provide desktop level protection against web threats. With this feature, users should warn and block access before accessing web pages with harmful content.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı web tehditlerine karşı desktop seviyesinde koruma sağlayacak olan web sitesi derecelendirme hizmet alabilmesini sağlamalıdır. Bu özellik ile kullanıcıların, zararlı içerikli olan web sayfalarına erişmeden önce uyarmalı ve erişim engellemesi sağlamalıdır.</i>
14.12.	In addition to malicious content sites that are blocked by the proposed Anti-Malware website rating feature, system administrators should be able to create their own allowed and banned lists.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı web sitesi derecelendirme özelliğinin engellediğı zararlı içerikli sitelere ek olarak, sistem yöneticileri, kendi izinli ve yasaklı listelerini oluşturabilmelidir.</i>
14.13.	The Malware Prevention Software to be offered should contain signatures and algorithms that can detect malicious codes, especially with different compression methods.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı özellikle farklı sıkıştırma metotları ile kendini içine saklayan zararlı kodları tespit edebilecek imzaları ve algoritmaları içerisinde barındırmalıdır.</i>
14.14.	The Anti-malware Software to be offered must include a stateful firewall.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı stateful özellikli bir güvenlik duvarı barındırmalıdır.</i>
14.15.	The firewall on the Anti-malware to be offered should protect against DoS attacks and Syn Flood attacks.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan güvenlik duvarı, DoS ataklarına, Syn Flood ataklarına karşı koruma sağlamalıdır.</i>
14.16.	All settings made on the proposed Anti-Malware Software should be backed up by the central management software and easily recycled from the previously purchased backup when necessary.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde yapılan tüm ayarlar merkezi yönetim yazılımı yolu ile yedeklenebilmeli ve gerektiğinde kolayca daha önce alınmış yedekten geri döndürülebilmelidir.</i>
14.17.	With the Malware Prevention Software to be offered, in case of a virus epidemic, shares and port access on the network should be closed with rules to be sent manually. Write rights on the file and folder should be able to be turned off.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile herhangi bir virüs salgını durumunda ağ üzerindeki paylaşımlar ve port erişimleri el ile yollanacak kurallarla kapatılabilmelidir. Dosya ve klasör üzerindeki yazma hakları kapatılabilmelidir.</i>

14.18.	With the Anti-malware Software to be offered, all virus, spyware and software updates should be done centrally and can be sent to clients remotely, automatically and manually.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile tüm virüs, spyware ve yazılım güncellemeleri merkezi olarak yapılmalı ve istemcilere uzaktan otomatik ve el ile yollanabilmelidir.</i>
14.19.	The Malware Prevention Software to be offered should have the infrastructure to ensure that the manually downloaded update files are applied to the central server even if the central server does not have an internet connection.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı merkezi sunucunun internet bağlantısı olmasa dahi el ile indirilen güncelleme dosyalarının merkezi sunucuya uygulanmasını sağlayacak alt yapıya sahip olmalıdır.</i>
14.20.	Anti-malware to be offered, mobile users should be able to keep their software under protection with their roaming profile when they are not connected to the center. At the same time, these users should be able to make updates via their internet connection without the need for central management software.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı mobil kullanıcılar merkez ile bağlantıları olmadığı zamanlarda gezici profili ile yazılımları koruma altında olmaya devam edebilmelilerdir. Aynı zamanda bu kullanıcılar merkezi yönetim yazılımına gerek kalmadan bulundukları internet bağlantısı yoluyla güncellemelerini yapabilmelilerdir.</i>
14.21.	With the Anti-malware to be offered, POP3 e-mail connections should also be able to be checked for malware.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile POP3 e-posta bağlantıları da zararlı yazılımlara karşı denetlenebilmelidir.</i>
14.22.	The Anti-malware Software to be offered should constantly monitor the activity on the computer whenever a file is opened or run, whenever any changes are made to the file (such as renaming, storing, moving, or copying to a directory or a directory) by looking at the virus signature definitions.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı bilgisayar üzerindeki aktiviteyi herhangi bir dosya açıldığında veya çalıştırıldığında, dosyada herhangi bir değişiklik yapıldığında (yeniden isimlendirme, saklama, taşıma veya bir dizine veya bir dizinden kopyalama gibi) virüs imza tanımlarına bakarak devamlı gözlemlemelidir.</i>
14.23.	Anti-malware to be offered, the user will be able to scan for viruses on usb disk, hard disk, CDROM, and network drives.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcı usb disk, hard disk, CDROM ve ağ sürücülerinde virüs taraması yapabilecektir.</i>
14.24.	Anti-malware to be offered will provide external device usage policies for users. There will be authorization rules for users to authorize the use of external devices.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcılar için harici aygıt kullanım politikaları sağlayacaktır. Kullanıcılar için harici aygıt kullanım yetkilendirilmesini sağlayan yetki kuralları mevcut olacaktır.</i>
14.25.	The Anti-malware Prevention Software to be offered will have heuristic scan feature. In this way, files that do not have a signature but are suspected of being viruses can be blocked.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı sezgisel tarama (heuristic scan) özelliğine sahip olacaktır. Bu sayede imzası bulunmayan ancak virüs olmasından şüphelenilen dosyalar bloklanabilecektir.</i>

14.26.	The Anti-malware Software to be offered will also check for viruses in compressed (zip, etc.) files.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı sıkıştırılmış (zip vb.) dosyalarda da virüs denetimi yapacaktır.</i>
14.27.	The Anti-malware Software to be offered should support the definition of exception rules so that the desired files and folders are not scanned during scans.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı taramalar sırasında istenilen dosya ve klasörlerin taranmaması için istisna kurallarının tanımlanmasını desteklemelidir.</i>
14.28.	The Malware Prevention Software to be offered should be able to alert the system administrator via e-mail if the threshold value determined in any virus outbreak or malicious code attacks on the network is exceeded.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı herhangi bir virüs salgını ya da ağ üzerinde yaşanan zararlı kod saldırılarında belirlenen eşik değeri geçilmesi durumunda sistem yöneticisini e-posta yoluyla uyaramelidir.</i>
14.29.	The Anti-malware to be offered should provide flexibility in processor (CPU) usage during security scans, and include maximum usage level settings.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı güvenlik taramaları sırasında işlemci (CPU) kullanımı konusunda esneklik sağlamalı, maksimum kullanım düzeyi ayarlarını içerisinde barındırmalıdır.</i>
14.30.	Anti-Malware user components to be offered must be able to be installed via MSI packages. MSI packages should be able to be modified and recreated with installation options.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcı bileşenleri MSI paketleri yoluyla kurulabilmelidir. MSI paketleri değiştirilebilmeli ve kurulum seçenekleri ile yeniden yaratılabilmelidir.</i>
14.31.	The Malware Prevention Software to be offered should support the installations of operating systems from the image.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile imajdan işletim sistemleri kurulumlarını desteklenmelidir.</i>
14.32.	The Anti-malware Software to be offered should support the reverting to previous versions of the virus update file and the malware scanning engine, both on the client and server side, in case of any problem. (Rollback)	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı herhangi bir sorun anında virüs güncelleme dosyasının ve zararlı tarama motorunun hem istemci hem de sunucu tarafında, bir önceki eski sürümlerine geri dönülmesini desteklemelidir. (Rollback)</i>
14.33.	Virus, system update, event log, instant virus scanning, etc. on the Anti-malware Management software to be offered. Event records of information should be kept. The storage duration of the event logs on the management software should be determined by the system administrator.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim yazılımı üzerinde virüs, sistem güncelleme, olay günlüğü, anlık virüs tarama vb. bilgilere ait olay kayıtları tutulmalıdır. Yönetim yazılımı üzerinde olay kayıtlarının saklanma süresi, sistem yöneticisi tarafından belirlenebilmelidir.</i>
14.34.	The Anti-malware Prevention Software to be offered will be automatically deleted from the system if inactive clients are detected within the specified day-out period.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı zaman aralığı verilerek belirlenen gün aşımında aktif olmayan istemciler tespit edildiği takdirde otomatik olarak sistemden silinmesi sağlanacaktır.</i>

14.35.	The Anti-malware to be offered should be able to alert the system administrator via e-mail and SNMP as soon as they are found malicious on clients.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı, istemciler üzerinde zararlı bulunduğu anda e-posta ve SNMP yoluyla sistem yöneticisini uyarabilmelidir.</i>
14.36.	It should be possible to specify how long the logs will remain in the system on the Anti-malware Prevention Software to be offered, and optimize the log records by defining the automatic deletion process .	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde üretilen logların sistemde ne kadar süre kalacağı belirtilebilmeli ve otomatik silme işlemi tanımlanarak log kayıtları üzerinde optimizasyon sağlanabilmelidir.</i>
14.37.	With the Malware Prevention Software to be offered, the management features of the software to be installed on the clients can be customized by the system administrator through the central management software. The removal of the software from memory should be prevented, and its removal from the system by uninstall should be secured with password protection. The system administrator should be able to block access to the folders where the client software is installed, as well as to deny access within the registry.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile istemcilere yüklenecek yazılımların yönetim özellikleri merkezi yönetim yazılımı yoluyla sistem yöneticisi tarafından özelleştirilebilecektir. Yazılımın hafızadan çıkarılması engellenebilmeli, uninstall ile sistemden kaldırılması şifre korumalı olarak güvenlik altına alınabilmelidir. Sistem yöneticisi isterse istemci yazılımının kurulduğu klasörlere erişimleri engelleyebileceği gibi kayıt defteri içindeki erişimlerini de kesebilmelidir.</i>
14.38.	Malware Prevention Software to be requested from the list of Spyware and Grayware should be considered as harmless and separated.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı Spyware ve Grayware listesinden istenilen yazılımlar zararsız olarak kabul edilip ayrıştırılabilmelidir.</i>
14.39.	The Anti-malware Software to be offered must support receiving updates via proxy.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı proxy üzerinden güncellemeleri almayı desteklemelidir.</i>
14.40.	Support the remote removal of agents located on endpoints with the Anti-malware Software to be offered.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile uç noktalar üzerinden bulunan ajanların uzaktan kaldırılmasını desteklemelidir.</i>
14.41.	The infected files quarantined with the Anti-malware Prevention Software to be offered should be encrypted and stored.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile karantinaya alınan virüslü dosyalar şifrelenerek saklanmalıdır.</i>
14.42.	More than one update source for the Anti-malware Software to be offered must be defined within the network. For this, an end-user computer with Malware Prevention Software agent installed on it should be used, and a separate computer should not be required for this feature.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı için birden fazla güncelleme kaynağı ağ içinde tanımlanabilmelidir. Bunun için üzerinde Zararlı Yazılım Önleme Yazılımı ajanı yüklü bir son kullanıcı bilgisayarı kullanılabilmesi, bu özellik için ayrı bir bilgisayar ihtiyacı olmamalıdır.</i>

14.43.	Anti-malware to be offered should be integrated into the central product management software of the same manufacturer as required.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı gerektiğinde aynı üreticinin merkezi ürün yönetim yazılımına entegre olmalıdır.</i>
14.44.	The Malware Prevention Software to be offered should be able to start time-dependent and instant scans on clients and monitor their results through the central management software.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı merkezi yönetim yazılımı yoluyla istemciler üzerinde zamana bağlı ve anlık taramalar başlatılıp sonuçları izlenebilmelidir.</i>
14.45.	The Anti-malware Software to be offered should scan the entire network from a single point, detect clients with and without antivirus software installed, and support the installation of an antivirus agent on clients that are not installed.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı tek noktadan tüm ağı tarayarak antivirüs yazılımı kurulu olan ve olmayan istemcileri tespit etmeli, kurulu olmayan istemcilere antivirüs ajanının kurulmasını desteklemelidir.</i>
14.46.	The Malware Prevention Software to be offered should support the monitoring method such as changing the system registry keys, changing the host file, installing a new service, and changing existing services within the pre-determined policies by monitoring the changes made by the software that can be run on the client, and these monitoring settings should be edited separately for a specific group or a single client.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı istemci üzerinde çalıştırılacak olan yazılımların sistem üzerinde yapacakları değişiklikleri izleyerek daha önceden belirlenecek politikalar dahilinde sistem kayıt defteri anahtarlarının değiştirilmesi, host dosyasının değiştirilmesi, yeni bir servis yüklenmesi ve var olan servislerin değiştirilmesi gibi izleme metodunu desteklemeli ve bu izleme ayarları tüm sistem, belirli bir grup veya tek bir istemci için ayrı ayrı düzenlenebilmelidir.</i>
14.47.	The Malware Prevention Software to be offered will be able to receive malicious URL, Domain, IP, and Hash information detected by the Detailed Analysis System for Advanced Attacks belonging to the same manufacturer as an update and share it with clients.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırıları için Detaylı Analiz Sistemi tarafından tespit edilen zararlı URL, Domain, IP ve Hash bilgisi güncelleme olarak alabilecek ve istemciler ile paylaşabilecektir.</i>
14.48.	The Malware Prevention Software to be offered will be able to receive the SHA-1 control summary information of the malicious software detected by the Detailed Analysis System for Advanced Attacks belonging to the same manufacturer as an update over the Security Management Software, and will be able to clean these malicious software through the infected clients.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırıları için Detaylı Analiz Sistemi tarafından tespit edilen zararlı yazılımların, şüpheli dosyaların SHA-1 kontrol özeti bilgilerini Güvenlik Yönetim Yazılımı üzerinden güncelleme olarak alabilecek ve bu zararlı yazılımları, şüpheli dosyaları bulaştığı istemciler üzerinden temizleyebilecektir.</i>

14.49.	The Malware Prevention Software to be offered will be able to send suspicious files extracted from USB, e-mail and web pages to the Detailed Analysis System for Advanced Attacks of the same manufacturer, regardless of whether the client is in or out of the institution, for detailed analysis.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırıları için Detaylı Analiz Sistemi'ne istemcinin kurum içinde ya da kurum dışında olmasından bağımsız olarak USB, e-posta ve web sayfalarından çekilmiş olan şüpheli dosyaları detaylı analiz amacı ile gönderebilecektir.</i>
14.50.	Proposed Anti-Malware Software will be able to transmit event logs to a SIEM solution via syslog.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı olay kayıtlarını syslog aracılığıyla bir SIEM çözümüne iletebilecektir.</i>
14.51.	Different administrator roles should be defined on the Anti-malware Prevention Software to be offered, and these users should be able to be pulled from Active Directory if desired.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde farklı yönetici rolleri tanımlanabilmeli ve bu kullanıcılar istenilirse Active Directory üzerinden çekilip kullanılabilir.</i>
14.52.	The Malware Prevention Software to be offered should be able to quickly generate detailed reports of the connected security software with ready report templates.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı hazır rapor şablonları ile hızlı bir şekilde bağlı bulunan güvenlik yazılımlarına ait detaylı raporlar üretebilmelidir.</i>
14.53.	Anti-malware to be offered will provide external device usage policies for users. There will be authorization rules for users to authorize the use of external devices.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcılar için harici aygıt kullanım politikaları sağlayacaktır. Kullanıcılar için harici aygıt kullanım yetkilendirilmesini sağlayan yetki kuralları mevcut olacaktır.</i>
14.54.	Special reports will be provided in the Anti-malware Prevention Software to be offered.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında özel raporlar alınması sağlanacaktır.</i>
14.55.	The Malware Prevention Software to be offered will be able to generate reports in pdf, docx , xlsx formats.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı pdf,docx,xlsx formatlarında rapor üretebilecektir.</i>
14.56.	Reports created with the Anti-malware Prevention Software to be offered should be able to be generated automatically depending on time.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile oluşturulan raporlar zamana bağlı olarak otomatik üretilmelidir.</i>
14.57.	The Malware Prevention Software to be offered should be able to transmit the automatically generated reports to predetermined people by e-mail.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı otomatik oluşturulan raporları e-posta ile daha önceden belirlenmiş kişilere iletebilmelidir.</i>
14.58.	The Anti-malware Software to be offered must have integrated data loss prevention (DLP) capability. • The data loss prevention	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı bütünleşmiş veri kaybı önleme özelliğine (DLP) sahip olmalıdır. • Teklif edilecek Zararlı Yazılım</i>

	system on the Anti-malware to be offered should have predefined data identifiers and templates and allow the identification of organization-specific identifiers and templates. • The data loss prevention system on the proposed Anti-Malware Software should be able to control access to certain applications and file types by default, and should be able to do this by recognizing the actual file type regardless of the file extension type. It should allow specific definitions for the institution to be made when necessary. • There must be a device control feature on the data loss prevention system on the Anti-malware Prevention Software to be offered. With this feature, data traveling from the client to different devices should be blocked, allowed or recorded according to the rules applied. • The data loss prevention system on the Anti-malware Prevention Software to be	<i>Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi ön tanımlı veri belirleyicileri ve şablonlara sahip olmalı ve kuruma özel belirleyici ve şablonların tanımlanmasına olanak tanımalıdır.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi ön tanımlı olarak belirli uygulama ve dosya tiplerine erişimi denetleyebilmeli, bu işlemi dosya uzantısı tipinden bağımsız olarak gerçek dosya tipini tanıyarak yapabilmelidir. Gerektiğinde kuruma özel tanımlamaların yapılmasına olanak sağlamalıdır.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi üzerinde cihaz kontrol özelliği bulunmalıdır. Bu özellik ile istemciden farklı cihazlara doğru giden veriler uygulanan kurallara göre engellenebilmeli, izin verilebilmeli ya da kayıt altına alınabilmelidir.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi aşağıda belirtilen veri çıkış kanallarını desteklemelidir.</i> • <i>Email Clients</i> • <i>FTP</i>
--	--	---

	offered must support the following data output channels. • Email Clients • FTP • HTTP and HTTPS • Instant communication applications (Instant Messaging) • SMB protocol • Webmail • Cloud storage services • CD / DVD • P2P applications • PGP encryption • Printer • External data storage • ActiveSync • Windows Clipboard	• HTTP ve HTTPS • Anlık haberleşme uygulamaları (Instant Messaging) • SMB protokolü • Webmail • Bulut depolama servisleri • CD/DVD • P2P uygulamaları • PGP şifreleme • Printer • Harici veri depolama • ActiveSync • Windows Clipboard
14.59.	The Malware Prevention Software to be offered will have an intrusion detection and prevention feature (HIPS) and a virtual patching feature against zero-day attacks.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında saldırı tespit ve engelleme özelliği (HIPS) ve sıfırcı gün ataklarına karşı sanal yama yapma özelliği bulunacaktır.</i>
14.60.	The Anti-malware to be offered will have an application control feature.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında uygulama kontrolü özelliği bulunacaktır.</i>
14.61.	With the "lockdown" feature in the application control in the Malware Prevention Software to be offered, it will be able to learn the user's current inventory and only allow them to prevent new applications from running.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde "lockdown" özelliği ile kullanıcının mevcut envanterini öğrenip sadece onlara izin vererek, yeni uygulamaların çalışmasını engelleyebilecektir.</i>
14.62.	Whitelist-blacklist rules can be created in the application control in the Anti-malware Prevention Software to be offered.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde whitelist-blacklist kurallar oluşturulabilecektir.</i>
14.63.	In the application control in the Malware Prevention Software to be offered, blocking / allowing rules can be written according to the HASH information of the applications.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde uygulamaların HASH bilgilerine göre bloklama/izin verme kurallar yazılabilecektir.</i>
14.64.	The application control included in the Anti-malware Prevention Software to be offered can only work in logging mode	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolü sadece loglama modunda çalışabilecektir.</i>

Item to be supplied description// <i>Tedarik edilecek ürün tanımı</i>		Quantity // <i>Miktar</i>
15. Uninterruptable Power Supply // <i>Kesintisiz Güç Kaynağı</i>		2 pieces // 2 adet
Technical Specifications		
15.1.	Bidding manufacturers must certify that they have the international ISO 9001-14001 and CE standard.	<i>Teklif veren üretici kuruluşlar Uluslararası ISO 9001-14001 ve CE standardına sahip olduklarını belgelemelidirler.</i>
15.2.	In order not to affect computers and sensitive electronic systems, it must comply with the EN 62040-2 (EMC) standard, which minimizes electromagnetic effects, and the EN 62040-1 standard, which includes safety items.	<i>Bilgisayar ve hassas elektronik sistemlerin etkilenmemesi bakımından, elektromanyetik etkileri minimuma indiren EN 62040-2 (EMC) standardına ve güvenlik maddelerini içeren EN 62040-1 standardına uygun olmalıdır</i>
15.3.	The offered product should be available in tower type and rack type when desired.	<i>Teklif edilen ürün istenildiğinde tower tip, istenildiğinde ise rack tipi kullanılabilir.</i>
15.4.	The company must provide the user manual and the service manual for maintenance and repair, written in Turkish language, free of charge, at the time of delivery of the UPSs, separately for each UPS.	<i>Firma KGK' ların teslimi anında, herbir KGK için ayrı ayrı olmak üzere, kullanıcı el kitabını ve bakım onarım için servis el kitabını, Türkçe dilinde matbaa harfleriyle yazılmış halde ücretsiz olarak vermelidir.</i>
15.5.	The UPSs will be an original model of the manufacturer's mass production. There will be no broken, cracked, scratched, paint defect, or deformed parts and will not be used.	<i>KGK 'lar imalatçının orijinal seri imalatı bir model olacaktır.Kırık, çatlak, çizik, boya hatası ve deformasyona uğramış hiçbir parçası bulunmayacak, kullanılmış olmayacaktır.</i>
15.6.	State-of-the-art materials and elements should be used in the manufacture of UPSs.	<i>KGK' ların imalatında son teknoloji ürünü malzeme ve elemanlar kullanılmalıdır.</i>
15.7.	All materials to be used in the assembly of UPSs must comply with TSE or international standards.	<i>KGK 'ların montajında kullanılacak tüm malzemeler TSE veya uluslararası standartlara uygun olmalıdır.</i>
15.8.	Must have SNMP module.	<i>SNMP modülü olmalıdır.</i>
15.9.	It should be able to be monitored with the Graphic Screen Remote Monitoring Panel when desired.	<i>İstenildiğinde Grafik ekranlı Uzaktan İzleme Paneli ile de izlenebilir.</i>
15.10.	Optionally, the MODBUS system must be compatible.	<i>Opsiyonel olarak MODBUS sistemi uyumlu olmalıdır.</i>
15.11.	The Uninterruptible Power Supplies offered must be designed online and with DSP Control.	<i>Teklif edilen Kesintisiz Güç Kaynakları online olarak tasarlanmış ve DSP Kontrollü olmalıdır.</i>
15.12.	The UPS must have a Boost charging	<i>KGK Boost şarj sistemine sahip olmalıdır.</i>

	system.	
15.13.	UPSs should give the output power in kVA clearly and continuously in the Technical specification.	<i>KGK'lar, Teknik şartname de kVA cinsinden verilen çıkış gücünü net ve sürekli olarak vermelidir.</i>
15.14.	UPS's; It should consist of rectifier, inverter, battery charger, static and manual by-pass switch main units.	<i>KGK 'lar; Redresör, İnvertör, Akü şarjörü, Statik ve Manuel By-pass Şalteri ana ünitelerinden oluşmalıdır.</i>
15.15.	The rectifier must have been manufactured using IPM technology. While providing the necessary DC voltage for the inverter, it should also be able to charge the batteries.	<i>Redresör IPM teknolojisi kullanılarak üretilmiş olmalıdır. İnvertör için gerekli DC gerilimi sağlarken aynı zamanda aküleri de şarj edebilmelidir.</i>
15.16.	The inverter must be manufactured using IGBT technology and must continuously feed the load by converting the DC energy received from the rectifier or battery pack into AC energy. The inverter should operate synchronously with the grid within the limits specified in the synchronization parameters. In case of inverter failure or overload, it should transfer the load to the grid without interruption in the load supply.	<i>İnvertör, IGBT teknolojisi kullanılarak imal edilmiş olmalıdır ve redresörden yada akü grubundan aldığı DC enerjiyi AC enerjiye çevirerek, sürekli olarak yükü beslemelidir. İnvertör, senkronizasyon parametrelerinde belirtilen sınırlar içinde şebekeye senkron çalışmalıdır. İnvertör arızasında veya aşırı yük durumunda, yük beslemesinde kesinti olmaksızın yükü şebekeye aktarmalıdır.</i>
15.17.	The battery pack must provide the necessary DC energy to the inverter in case the mains fails or the grid goes out of the specified tolerance. In case the network returns or returns within limits, the rectifier should automatically supply DC energy and the battery charger should start charging the battery group.	<i>Şebekenin kesildiği veya şebekenin belirtilen tolerans dışına çıkması durumunda akü grubu invertöre gerekli DC enerjiyi sağlamalıdır. Şebekenin geri gelmesi veya limitler içine dönmesi durumunda, redresör otomatik olarak DC enerjiyi sağlamalı, akü şarjörü akü grubunu şarj etmeye başlamalıdır.</i>
15.18.	In order to save energy in the proposed uninterruptible power supplies, economical operating mode (Ecomode) should be optional.	<i>Teklif edilen Kesintisiz güç kaynaklarında enerji tasarrufu amacıyla opsiyonel olarak ekonomik çalışma modu (Ecomode) olmalıdır.</i>
15.19.	In case of failure, the UPS should be able to disable itself depending on the location and nature of the failure. The faults should be visible on the panel on the UPS with the illuminated LEDs or on the LCD panel.	<i>Arıza durumunda, arızanın yerine ve mahiyetine göre KGK kendisini devre dışı bırakabilmelidir. Arızalar KGK üzerindeki panelden ışıklı LED 'lerle veya LCD panel üzerinden görülebilmelidir.</i>
15.20.	128 historical events and 5000 alarms must be able to be kept in the memory.	<i>Geçmişe yönelik 128 adet olay ve 5000 alarmı hafızada tutulabilmelidir.</i>

15.21.	There should also be a manual by-pass unit in order to facilitate maintenance operations.	<i>Bakım işlemlerinde kolaylık sağlaması amacıyla ayrıca manuel by-pass ünitesi de bulunmalıdır.</i>
15.22.	In order to facilitate maintenance / repair and minimize maintenance time, UPS's microprocessor circuits and circuit boards should be in easily accessible locations and in a replaceable manner in case of malfunction.	<i>Bakım/onarımın kolaylaştırılması ve bakım süresinin asgari seviyeye indirilmesi amacıyla KGK'ların mikroişlemci devreleri ile devre kartları kolay ulaşılabilir yerlerde ve arıza durumunda değiştirilebilir şekilde olmalıdır.</i>
15.23.	UPS must be working in parallel at least up to 4 units.	<i>KGK' en az 4 adete kadar paralel çalışıyor olmak zorundadır.</i>
15.24.	The technical service has to present the training certificates in the offer attachment.	<i>Teknik servisin eğitim sertifikalarını teklif ekinde sunmak zorundadır.</i>
15.25.	Input characteristics • Input Voltage and Tolerance : 220VAC (1Phase N) $\pm$ 20% • Input Frequency and Tolerance : 40-65hz • Bypass voltage and Tolerance : the first phase 220 $\pm$ 10% • System Input Power Factor : 0.99 • Input Current THD : <5%	<i>Giriş karakteristikleri</i> • Giriş Gerilim ve Toleransı :220VAC (1FAZ, N) $\pm$ %20 • Giriş Frekansı ve Toleransı :40-65Hz • By-Pass Gerilimi ve Toleransı :220 1 faz $\pm$ %10 • Sistem Giriş Güç Faktörü :0,99 • Giriş Akım THD :<%5
15.26.	Output Characteristics • Output Power : 15 kVA • Power Kw : 10.5 kW • Output Waveform : sinusoidal • Output Voltage : 220 VAC • Output Voltage Tolerance : +/- 1% • Output Power Factor : 0.7 • Output Frequency : 50 Hz • Output Frequency Tolerance : +/- %0.2 • Efficiency at 100% load :> 92% • Crest Factor : 3: 1 • Overload : 10 minutes at 100-125% load. • Output Voltage at Linear Load : <3% • Acoustic Noise : <50 dBA	<i>Çıkış Karakteristikleri</i> • Çıkış Gücü :15 kVA • Güç Kw :10.5 kW • Çıkış Dalga Şekli : Sinusoidal • Çıkış Gerilimi : 220 VAC • Çıkış Gerilim Toleransı : +/- %1 • Çıkış Güç Faktörü : 0,7 • Çıkış Frekansı : 50 Hz • Çıkış Frekans Toleransı : +/- %0.2 • Verim %100 yükte :>%92 • Crest Faktörü : 3:1 • Aşırı Yük : %100-125 yükte 10 dk. • Çıkış Gerilimi Lineer Yükte : < %3 • Akustik Gürültü : < 50 dba
15.27.	It must be in a structure that can keep the battery group in float charge while feeding the inverter at full load by converting the one-phase alternating voltage received from the network to the regulated correct voltage.	<i>Şebekeden aldığı bir fazlı alternatif gerilimi regüle edilmiş doğru gerilime çevirerek invertörü tam yükte beslerken akü grubunu tampon şarjda tutabilecek yapıda olmalıdır.</i>
15.28.	The rectifier must have soft start	<i>Redresör soft start özelliğine sahip olmalıdır.</i>

	feature. The current drawn during soft start should not be more than the rated current of the device. Even if the input voltage is cut for a very short time (the situation where the rectifier DC bus does not reach zero completely), it should draw current in accordance with the soft start feature.	<i>Soft start esnasında çekilen akım cihazın anma akımından fazla olmamalıdır. Giriş geriliminin çok kısa süreli kesilmesinde dahi (doğrultucu DC barasının tamamen sıfıra erişmediği durum) soft start özelliğine uygun akım çekmelidir.</i>
15.29.	In case of mains power cut, input voltage and frequency out of specified tolerance values, and in cases such as phase cut, the rectifier will be automatically deactivated and the inverter will be fed through the battery . In case the appropriate voltage and frequency to be provided from the network or generator is restored, the rectifier will automatically re-engage and feed the inverter.	<i>Şebeke enerjisinin kesilmesinde, giriş gerilim ve frekansının belirtilen tolerans değerleri dışına çıkmasında ve faz kesilmesi gibi durumlarda redresör otomatik olarak devreden çıkacak, invertör akü üzerinden beslenecektir. Şebeke veya jeneratörden sağlanacak uygun gerilim ve frekansın yeniden sağlanması durumunda redresör otomatik olarak tekrar devreye girerek invertörü besleyecektir.</i>
15.30.	In order to prevent the battery cells from being damaged by excessive charging current, there will be a current limiting circuit on the charge card.	<i>Akü hücrelerinin aşırı şarj akımı ile hasarlanmasının önlenmesi amacıyla, şarj kartında akım sınırlama devresi bulunacaktır.</i>
15.31.	Designed using IPM technology, the inverter must transfer the DC voltage from the rectifier or battery pack to a regulated and noise-free AC voltage and transfer it to the static transfer circuit.	<i>IPM teknolojisi kullanılarak tasarlanan invertör, redresör veya akü grubundan gelen DC gerilimi regüleli ve her türlü gürültüden arındırılmış bir AC gerilime çevirerek statik transfer devresine aktarmalıdır.</i>
15.32.	The inverter should be manufactured as microprocessor controlled so that it will be continuously on.	<i>İnvertör sürekli olarak devrede kalacak şekilde mikro işlemci kontrollu olarak imal edilmiş olmalıdır.</i>
15.33.	Output voltage should not exceed +/- 1% and frequency +/- 0.2 % (battery operation) tolerance limits.	<i>Çıkış gerilimi +/- %1 ve frekansı +/- %0.2 (Aküden çalışma) tolerans sınırlarını aşmamalıdır.</i>
15.34.	The dynamic tolerance of the output voltage should not exceed +/- 5%. (At 100% load impulse) This tolerance should be set to $\pm 2\%$ within 20 ms at the most.	<i>Çıkış geriliminin dinamik toleransı +/- %5 'i aşmamalıdır. (% 100 yük darbesinde) Bu tolerans en çok 20 msn'de $\pm 2\%$ sınırlarına çekilmelidir.</i>
15.35.	Total harmonic amount of output voltage at full load should not exceed 3% in linear loads and 5% in computer loads (CF: 3: 1).	<i>Tam yükte çıkış gerilimi toplam harmonik miktarı, lineer yüklerde % 3'ü, bilgisayar yüklerinde (CF: 3:1) %5 'ü geçmemelidir.</i>
15.36.	The inverter output must be protected against short circuits.	<i>İnvertör çıkışı kısa devrelere karşı korunmuş olmalıdır.</i>

15.37.	The inverter must have an overheat protection circuit.	<i>İnvertörde aşırı ısı koruma devresi bulunmalıdır.</i>
15.38.	It must be an electronically controlled semiconductor switch consisting of semi-conductors and feed the load from the inverter in the normal operation of the UPS. In case of overload, short circuit, or a failure in the inverter, the load should be transferred to the network or auxiliary source without power cut. If the inverter also fails, it must transfer the load back to the inverter. If it is out of the specified tolerance value, it should not transfer to the network.	<i>Yarı iletkenlerden meydana gelen elektronik kontrollü yarı iletken bir şalter olmalı ve KGK ' nın normal çalışması durumunda yükü invertörden beslemelidir. Aşırı yükte, kısa devre durumunda veya invertörde bir arıza meydana geldiğinde yükü enerji kesintisi olmaksızın şebekeye yada yardımcı kaynağa aktarmalıdır. Invertör de arıza geçmiş ise yükü tekrar invertöre aktarmalıdır. Belirlenen tolerans değeri dışında ise şebekeye transfer işlemini gerçekleştirmemelidir.</i>
15.39.	As long as the grid is within the given tolerance limits, it should be able to perform automatic synchronization and phase locking with the inverter output. Otherwise, the inverter should be locked to its internal oscillator.	<i>Şebeke verilen tolerans sınırları içinde olduğu sürece invertör çıkışı ile aralarında otomatik senkronizasyon ve faz kilitlemesi yapabilmelidir. Aksi durumda invertör kendi dahili osilatörüne kilitlenmelidir.</i>
15.40.	From the LEDs on the front panel of the UPS or the LCD screen, it should be possible to learn whether the mains and the inverter output are synchronous , synchronous out-of-limit status and overload status.	<i>UPS ön panelindeki ledler veya LCD ekrandan, şebeke ile invertör çıkışının senkron olup olmadığını, senkron limit dışı durumunu ve aşırı yük durumunu öğrenilebilmelidir.</i>
15.41.	Static transfer circuit should be able to automatically select the network or inverter under specified conditions. In synchronous operation, the transfer between the inverter and the grid should be possible without interruption.	<i>Statik transfer devresi belirtilen şartlarda şebeke veya invertör seçimini otomatik olarak yapabilmelidir. Senkron çalışmada, invertör ile şebeke arasındaki transfer kesintisiz yapılabilirdir.</i>
15.42.	When the UPS is requested to be disabled for maintenance, repair, or other reasons, it should transfer the load to the network or auxiliary source without interruption.	<i>Bakım, onarım veya başka sebeplerle KGK ' nın devre dışı bırakılması istenildiğinde yükü şebekeye yada yardımcı kaynağa kesintisiz aktarmalıdır.</i>
15.43.	When this switch is ON, there should be no voltage at any point in the UPS cabinet other than the input terminals.	<i>Bu şalter ON durumunda iken KGK kabini içerisinde giriş terminallerinin dışında hiçbir noktada gerilim bulunmamalıdır.</i>
15.44.	When 220/380 V, 50 Hz mains power is cut or when the specified tolerance band is exceeded, the UPS should continue to supply the load from the dual polarity battery group. It should	<i>220/380 V, 50 Hz şebeke enerjisi kesildiğinde yada belirtilen tolerans bandının dışına çıktığında KGK çift polariteli akü grubundan yükü beslemeye devam etmelidir. Beslenecek sistemi tam yükte 15 dk süreyle</i>

	feed the system to be fed for 15 minutes at full load. No interruption should be felt in the output from the battery group to supply.	<i>beslemelidir. Akü grubundan beslemeye geçişte, çıkışta herhangi bir kesinti hissedilmemelidir.</i>
15.45.	Batteries; completely closed, maintenance-free, dry type, stationary (suitable for being under continuous charging) rechargeable, must have a life expectancy of at least 5 years.	<i>Aküler; tamamen kapalı, bakım gerektirmeyen (maintenance-free), kuru Tip, stasyonier (sürekli şarj altında kalmaya elverişli) şarj edilebilen, en az 5 yıl ömür beklentili olmalıdır.</i>
15.46.	Information such as battery capacity used, battery charge voltage, and current should be monitored on the LCD panel on the device and from the software.	<i>Kullanılan akü kapasitesi , akü şarj voltajı ve akımı gibi bilgilerin cihazın üzerindeki LCD panelden ve yazılımdan izlenebilmelidir.</i>
15.47.	Batteries necessary for the maintenance of the UPS System ' from separating switching system will be found. In this state, the UPS should continue to perform its functions without a battery.	<i>Sistemin bakımı için gerektiğinde aküleri KGK 'dan ayıran anahtarlama sistemi bulunacaktır. Bu durumda iken KGK aküsüz olarak fonksiyonlarını yerine getirmeye devam etmelidir.</i>
15.48.	The calculation of the battery group should be made using the maximum power per cell method.	<i>Akü grubunun hesabı hücre başına düşen maksimum güç yöntemiyle yapılmalıdır.</i>
15.49.	Battery connection parts will be insulated and not touch the body. Connections between blocks should be made of flexible material.	<i>Akü bağlantı parçaları izoleli ve gövdeye temas etmeyecek şekilde olacaktır. Bloklar arası bağlantılar esnek malzemeden yapılmalıdır.</i>
15.50.	Rectifier, Bypass inputs, and Inverter output must be protected with a breaker or fuse in the system.	<i>Sistemde Doğrultucu, Bypass girişleri ve Evirici çıkışı şalter veya sigorta ile korunmalıdır.</i>
15.51.	The inverter must be electronically protected against overload and short circuits.	<i>Aşırı yük ve kısa devreye karşı evirici elektronik olarak korunmalıdır.</i>
15.52.	The system must have battery overcharge and discharge protection.	<i>Sistem, akü aşırı şarj ve deşarj korumasına sahip olmalıdır.</i>
15.53.	The system must have over-heat protection.	<i>Sistem aşırı ısı korumasına sahip olmalıdır.</i>
15.54.	The user should be able to access information about the operation of the system through the control panel of the UPS or the LCD screen. In addition, there should be a sound warning that can be silenced in case of failure or power failure.	<i>KGK' nın kontrol paneli veya LCD ekran üzerinden, kullanıcı sistemin çalışması ile ilgili bilgilere ulaşabilmelidir. Ayrıca arıza veya elektrik kesintisi durumunda susturulabilir ses ikazı olmalıdır.</i>
15.55.	A connection with a computer must be possible with a standard RS 232 output.	<i>Standart RS 232 çıkışı ile bilgisayar'la bağlantı kurulabilmelidir. KGK ile ilgili tüm</i>

	All information about the UPS should be displayed on the screen.	<i>bilgiler ekrandan izlenebilmelidir.</i>
15.56.	As standard, the UPS should automatically shut down Novell, Windows, NT type operating systems when the electricity is cut off. The software to be provided for these operating systems must be graphic-based and given free of charge.	<i>Standart olarak UPS elektrikler kesildiğinde Novell, Windows, NT, tipi işletim sistemlerini otomatik kapatabilmelidir. Bu işletim sistemleri için verilecek yazılım grafik tabanlı olmalı ve ücretsiz olarak verilmelidir</i>
15.57.	The UPS must be compatible to be used with SNMP and communication must be made with SNMP when required.	<i>KGK SNMP ile kullanılmaya uyumlu olmalı ve istenildiğinde haberleşme SNMP ile yapılabilinmelidir.</i>
15.58.	The UPS system must have a firmware structure so that the system must be fully software controlled. Future developments should be able to be transferred to the system with the software development function and the system should be updated.	<i>KGK sistemi firmware yapısına sahip olmalı böylece sistem tamamı ile yazılım kontrollü olmalıdır. İleride olabilecek gelişmeler yazılım geliştirme fonksiyonu ile ile sisteme aktarılabilinmeli ve sistem update edilebilmelidir.</i>
15.59.	It should have automatic and manual battery test feature.	<i>Otomatik ve manuel akü test özelliği olmalıdır.</i>
15.60.	The Uninterruptible Power Supply must be able to operate continuously between 0 °C and 40 °C, The working altitude must be up to 1000 m and at higher levels the system must operate with excessive air circulation .	<i>Kesintisiz GüçKaynağı 0°C ile 40°C arasında sürekli çalışabilmeli, Çalışma yüksekliği 1000 m'ye kadar olmalı ve daha yukarı seviyelerde sistem, fazla hava sirkülasyonu sağlamakla çalışmalıdır.</i>
15.61.	The amount of heat the system emits into the environment should be specified.	<i>Sistemin ortama yaymakta olduğu ısı miktarı belirtilmelidir.</i>
15.62.	The Uninterruptible Power Supply should have a front panel in liquid crystal display (LCD) structure.	<i>Kesintisiz Güç Kaynağında likit kristal display (LCD) yapısında bir ön panel bulunmalıdır.</i>
15.63.	The user should be able to get information about the progress of the system at a glance from this panel. Control keys and other controller keys required for the system should also be located here.	<i>Kullanıcı bu panodan sistemin gidişatı hakkında bir bakışta bilgi sahibi olabilmelidir. Sistem için gerekli olan kontrol tuşları ile diğer kontrol edici anahtarlar da burada yer almalıdır.</i>
15.64.	The following status and alarm messages must be visible on the front panel: • Load is on Uninterruptible Power Supply • Freight By-Pass also • Manual By-Pass	<i>Ön panelde aşağıdaki durum ve alarm mesajları mutlaka görülebilmelidir:</i> • <i>Yük Kesintisiz Güç Kaynağında</i> • <i>Yük By-Pass da</i> • <i>Manuel By-Pass</i> • <i>Acil kapatma</i> • <i>Akü gerilimi düşük</i> • <i>Arıza kodları</i>

	• Emergency shutdown • The battery voltage is low • Fault codes • Audible alarm on • Mains cut • Overload • Excessive heat • Battery low • High Battery • Output low • Output high	• <i>Sesli alarm açık</i> • <i>Şebeke kesik</i> • <i>Aşırı yük</i> • <i>Aşırı ısı</i> • <i>Akü düşük</i> • <i>Akü yüksek</i> • <i>Çıkış düşük</i> • <i>Çıkış yüksek</i>
15.65.	In addition, the values below should be monitored on the LCD panel from the measurement menu: • Load value in% • Output voltage and frequency • Input voltage, current, and frequency • By-pass voltage and frequency • Input current • Battery voltage, battery discharge current • Battery capacity and remaining battery time • Temperature	<i>Ayrıca aşağıda bulunan değerler ölçüm menüsünden LCD panelde izlenebilmelidir.</i> • <i>% olarak yük değeri</i> • <i>Çıkış voltajı ve frekansı</i> • <i>Giriş voltajı, akımı ve frekansı</i> • <i>By-pass voltajı ve frekansı</i> • <i>Giriş akımı</i> • <i>Akü voltajı , şarj deşarj akımı</i> • <i>Akü kapasitesi ve kalan akü süresi</i> • <i>Sıcaklık</i>

Section 5b: Other Related Requirements

Further to the Schedule of Requirements in the preceding Table, Bidders are requested to take note of the following additional requirements, conditions, and related services pertaining to the fulfillment of the requirements:

Delivery Term	Turnkey delivery in the address stipulated in the ITB.
Exact Address of Delivery/Installation Location	İzmir Model Factory Fatih Mahallesi Ege Cad. No 39/4 Sarnıç Gaziemir 35410 İzmir / TURKEY The bidders shall include all types of costs to be incurred until turnkey delivery and installation of the items at above stated location, in their bid prices. No additional payment over and above the bid price of the successful bidder shall be made.
Delivery Time	Delivery and installation shall be completed, and the items shall be in a proper working condition and ready for the inspection within 90 calendar days after signature of the contract by UNDP and the Contractor.
Installation Requirements	Configuration and installation of the whole system with all accessories shall be completed by the contractor on a turnkey basis and all cost related to configuration and installation of items shall be included in the bid price. Installation of the products shall be carried out by at least 2 company engineers in order to guarantee backup and to prevent possible disruptions in the delivery. No payment will be made separately for installation of items.
Testing Requirements	UNDP or its designated inspection agents will inspect the goods upon delivery in order to confirm that the goods conform to applicable specifications or other requirements of the Contract.
Inspection upon delivery	All the equipment shall be provided complete with the necessary accessories (network cables, power cables, power adapter etc.) and/or parts such as to ensure that the unit is capable of operating to the required technical and quality specifications. System components and whole system must be compatible with each other (i.e. there should not be any interoperability problems among different components of the system, hardware and software). In addition to the Article 11 "Purchase of Goods" of Annex 3- General Terms and Conditions for Contracts, inspection and acceptance procedures shall be carried out by the Inspection and Acceptance Committee following the delivery, installation and commissioning of goods. At the end of the inspections, UNDP has the right to not

	release to the Contractor any payments in the event that the Inspection and Acceptance Committee detects incomplete and/or improper work in accordance with the Technical Specifications, including but not limited to proper functioning or poor performance of the whole system.
Scope of Training on Operation and Maintenance	Pursuant to UNDP's positive Inspection and Acceptance Report, the Contractor shall give training on the operation of the whole system and equipment to the beneficiary/end user on date and address to be notified by UNDP. Training related costs shall be factored into the bid price, and no additional payment over and above the bid price shall be made to the Contractor due to trainings.
Warranty Period	All items shall have certified three years manufacturer warranty certified with a warranty certificate in accordance with the Regulation on Code of Practice for Warranty Certificate. Any hardware and whole systems that are announced as end-of-line by the manufacturer shall not be proposed by the offeror. Response Time: During warranty period, in any case resulting from deficiency or any other problem of the goods, the Contractor shall troubleshoot within 4 hours (online or via phone). If the problem cannot be solved online or via phone support, Contractor shall be available or act on site within 24 hours. Repair Time: In the case of the failure of any product due to material, workmanship, or assembly errors during the warranty period; the contractor is responsible to repair the product without requesting any additional payment within 20 working days. If the repair is impossible, the contractor shall provide a new product which has the same properties as the failed one within 2 weeks. If this is also impossible, the contractor is responsible for providing a new product that has specifications exceeding the failed one with the approval of the end user/beneficiary within one month duration.
Local Service Support	Must be available. The bidders shall explain in detail in their bids the scope and means of local service support they will provide in case awarded by the contract.
After Sales Services	The Contractor and manufacturer/distributor shall guarantee after sales service and spare parts supply during the economic life of machines determined by the Revenue Administration of Turkey (GIB). Please refer to https://www.gib.gov.tr/fileadmin/user_upload/Yararli_Bilgiler/_amortisman_oranlari.pdf for economic life of machines. After completion of the inspection and the acceptance, full title and ownership of the asset will be transferred to the end

	user and the contractor will be directly responsible towards the end user for after sales services
Payment Terms <i>(max. advanced payment is 20% as per UNDP policy)</i>	100% within 30 days upon UNDP's issuance of Positive Inspection and Acceptance Report that indicates full compliance of the goods to Technical Specifications in this ITB and proper functioning of the whole system and receipt of invoice.
Conditions for Release of Payment	☒ Inspection upon arrival at destination ☒ Installation and Commissioning ☒ Testing ☒ Training on Operation and Maintenance ☒ Written Acceptance of Goods based on full compliance with ITB requirements
All documentations, including catalogues, instructions and operating manuals, shall be in this language	English/Turkish
Documents to be provided prior to acceptance	Signed and stamped warranty certificate for each item Application and User Manual Document indicating that the product is an output of the Authorized Distributor for each product

Section 6: Returnable Bidding Forms / Checklist

This form serves as a checklist for preparation of your Bid. Please complete the Returnable Bidding Forms in accordance with the instructions in the forms and return them as part of your Bid submission. No alteration to format of forms shall be permitted and no substitution shall be accepted.

Before submitting your Bid, please ensure compliance with the Bid Submission instructions of the BDS 22.

Technical Bid:

Have you duly completed all the Returnable Bidding Forms?	
▪ Form A: Bid Submission Form	☐
▪ Form B: Bidder Information Form	☐
▪ Form D: Qualification Form	☐
▪ Form E: Format of Technical Bid	☐
▪ Form G: Form of Bid Security	☐
Have you provided the required documents to establish compliance with the evaluation criteria in Section 4?	☐

Price Schedule:

▪ Form F: Price Schedule Form	☐
-------------------------------	--------------------------

Form A: Bid Submission Form

Name of Bidder:	[Insert Name of Bidder]	Date:	Select date
ITB reference:	[Insert ITB Reference Number]		

We, the undersigned, offer to supply the goods and related services required for [Insert Title of goods and services] in accordance with your Invitation to Bid No. [Insert ITB Reference Number] and our Bid. We hereby submit our Bid, which includes this Technical Bid and Price Schedule.

Our attached Price Schedule is for the sum of [Insert amount in words and figures and indicate currency].

We hereby declare that our firm, its affiliates or subsidiaries or employees, including any JV/Consortium /Association members or subcontractors or suppliers for any part of the contract:

- a) is not under procurement prohibition by the United Nations, including but not limited to prohibitions derived from the Compendium of United Nations Security Council Sanctions Lists;
- b) have not been suspended, debarred, sanctioned or otherwise identified as ineligible by any UN Organization or the World Bank Group or any other international Organization;
- c) have no conflict of interest in accordance with Instruction to Bidders Clause 4;
- d) do not employ, or anticipate employing, any person(s) who is, or has been a UN staff member within the last year, if said UN staff member has or had prior professional dealings with our firm in his/her capacity as UN staff member within the last three years of service with the UN (in accordance with UN post-employment restrictions published in ST/SGB/2006/15);
- e) have not declared bankruptcy, are not involved in bankruptcy or receivership proceedings, and there is no judgment or pending legal action against them that could impair their operations in the foreseeable future;
- f) undertake not to engage in proscribed practices, including but not limited to corruption, fraud, coercion, collusion, obstruction, or any other unethical practice, with the UN or any other party, and to conduct business in a manner that averts any financial, operational, reputational or other undue risk to the UN and we embrace the principles of the United Nations Supplier Code of Conduct and adhere to the principles of the United Nations Global Compact.

We declare that all the information and statements made in this Bid are true and we accept that any misinterpretation or misrepresentation contained in this Bid may lead to our disqualification and/or sanctioning by the UNDP.

We offer to supply the goods and related services in conformity with the Bidding documents, including the UNDP General Conditions of Contract and in accordance with the Schedule of Requirements and Technical Specifications.

Our Bid shall be valid and remain binding upon us for the period specified in the Bid Data Sheet.

We understand and recognize that you are not bound to accept any Bid you receive.

I, the undersigned, certify that I am duly authorized by [Insert Name of Bidder] to sign this Bid and bind it should UNDP accept this Bid.

Name: _____

Title: _____

Date: _____

Signature: _____

[Stamp with official stamp of the Bidder]

Form B: Bidder Information Form

Legal name of Bidder	[Complete]
Legal address	[Complete]
Year of registration	[Complete]
Bidder's Authorized Representative Information	Name and Title: [Complete] Telephone numbers: [Complete] Email: [Complete]
Are you a UNGM registered vendor?	☐ Yes ☐ No If yes, [insert UGNM vendor number]
Are you a UNDP vendor?	☐ Yes ☐ No If yes, [insert UNDP vendor number]
Countries of operation	[Complete]
No. of full-time employees	[Complete]
Quality Assurance Certification (e.g. ISO 9000 or Equivalent) <i>(If yes, provide a Copy of the valid Certificate):</i>	[Complete]
Does your Company hold any accreditation such as ISO 14001 or ISO 14064 or equivalent related to the environment? <i>(If yes, provide a Copy of the valid Certificate):</i>	[Complete]
Does your Company have a written Statement of its Environmental Policy? <i>(If yes, provide a Copy)</i>	[Complete]
Does your organization demonstrates significant commitment to sustainability through some other means, for example internal company policy documents on women empowerment, renewable energies or membership of trade institutions promoting such issues	[Complete]
Is your company a member of the UN Global Compact	[Complete]
Contact person that UNDP may contact for requests for	Name and Title: [Complete]

clarifications during Bid evaluation	Telephone numbers: [Complete] Email: [Complete]
Please attach the following documents:	▪ Certificate of Incorporation/ Business Registration ▪ Trade name registration papers, if applicable ▪ Signature Circular/Power of Attorney ▪ Certification or authorization to act as agent / dealer / distributor on behalf of the Manufacturer ▪ Export Licenses, if applicable ▪ Official Letter of Appointment as local representative, if Bidder is submitting a Bid on behalf of an entity located outside the country

Form D: Eligibility and Qualification Form

Name of Bidder:	[Insert Name of Bidder]	Date:	Select date
ITB reference:	[Insert ITB Reference Number]		

History of Non- Performing Contracts

☐ Non-performing contracts did not occur during the last 3 years			
☐ Contract(s) not performed in the last 3 years			
Year	Non- performed portion of contract	Contract Identification	Total Contract Amount (current value in USD)
		Name of Client: Address of Client: Reason(s) for non-performance:	

Litigation History (including pending litigation)

☐ No litigation history for the last 3 years			
☐ Litigation History as indicated below			
Year of dispute	Amount in dispute (in TRY)	Contract Identification	Total Contract Amount (current value in USD)
		Name of Client: Address of Client: Matter in dispute: Party who initiated the dispute: Status of dispute: Party awarded if resolved:	

Previous Relevant Experience

Please list only previous similar assignments successfully completed in the last 3 years.

List only those assignments for which the Bidder was legally contracted by the Client as a company or was one of the Consortium/JV partners. Assignments completed by the Bidder's individual experts working privately or through other firms cannot be claimed as the relevant experience of the Bidder, or that of the Bidder's partners or sub-consultants, but can be claimed by the Experts themselves in their CVs. **The Bidder shall provide proof documents for the claimed experience by presenting copies of relevant documents and references with the Bid.**

Project name & Country of Assignment	Client & Reference Contact Details	Contract Value (in USD equivalent*)	Period of activity and status	Types of activities undertaken

**Bidders shall convert the currency quoted in the "Certificate of Completion" into USD, in accordance with the*

prevailing UN operational rate of exchange on the contract date stated by “Certificate of Completion”. UN operational rate of exchange are available at the following website: <https://treasury.un.org/operationalrates/OperationalRates.php#E>

Bidders may also attach their own Project Data Sheets with more details for assignments above.

Bidders shall submit Statements of Satisfactory Performance (i.e. Reference Letters, Work Completion Certificates) along with their bids. Reference letters and/or Completion Certificates shall include the information requested in above table at minimum.

Financial Standing

Annual Turnover for the last 3 years	Year	USD
	Year	USD
	Year	USD
Latest Credit Rating (if any), indicate the source		

Financial information (in USD equivalent)	Historic information for the last 3 years		
	Year 1	Year 2	Year 3
	<i>Information from Balance Sheet</i>		
Total Assets (TA)			
Total Liabilities (TL)			
Current Assets (CA)			
Current Liabilities (CL)			
	<i>Information from Income Statement</i>		
Total / Gross Revenue (TR)			
Profits Before Taxes (PBT)			
Net Profit			
Current Ratio			

For USD Equivalent: Bidders shall convert the currency into USD by using the UN operational rate of exchange which was effective for 31st December of each corresponding year. UN operational rate of exchange are available at the following website: <https://treasury.un.org/operationalrates/OperationalRates.php#E>

Bidders shall submit copies of the audited financial statements (balance sheets, including all related notes, and income statements) for the years required above complying with the following condition: Must reflect the financial situation of the Bidder or party to a JV, and not sister or parent companies;

- Historic financial statements must be audited by a certified public accountant;
- Historic financial statements must correspond to accounting periods already completed and audited. No statements for partial periods shall be accepted.

Form E: Format of Technical Bid

Name of Bidder:	[Insert Name of Bidder]	Date:	Select date
ITB reference:	[Insert ITB Reference Number]		

The Bidder's Bid should be organized to follow this format of the Technical Bid. Where the bidder is presented with a requirement or asked to use a specific approach, the bidder must not only state its acceptance, but also describe how it intends to comply with the requirements. Where a descriptive response is requested, failure to provide the same will be viewed as non-responsive.

SECTION 1: Bidder's qualification, capacity and expertise

- 1.1 General organizational capability which is likely to affect implementation: management structure, financial stability and project financing capacity, project management controls, extent to which any work would be subcontracted (if so, provide details).
- 1.2 Relevance of specialized knowledge and experience on similar engagements done in the region/country.

SECTION 2: Scope of Supply, Technical Specifications, and Related Services

This section should demonstrate the Bidder's responsiveness to the specification by identifying the specific components proposed, addressing the requirements, as specified, point by point; providing a detailed description of the essential performance characteristics proposed; and demonstrating how the proposed bid meets or exceeds the requirements/specifications. All important aspects should be addressed in sufficient detail.

IMPORTANT NOTE:

Bidders shall fill out below table in English by indicating the Brand Name and Model number of the products offered as well as the specifications of the offered products corresponding to the specifications listed in below table. If the offered product does not meet any of below minimum technical specifications, it will not be considered to be compliant and the offer will be disqualified. Please ensure that the offered product meets the minimum specifications requested below.

#	Item to be supplied description	<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
1.	Server	<i>Sunucu</i>	Brand/Model // <i>Marka/Model:</i>
1.1	Each processor must support a 64-bit set of commands.	<i>Her bir işlemci 64-bit komut setini desteklemelidir.</i>	
1.2	There must be at least 2 physical processors on the	<i>Sunucu üzerinde en az 2 adet, en az 3.7 GHz çalışma hızında</i>	

	server with an operating speed of at least 3.7 GHz.	<i>fiziksel işlemci olmalıdır.</i>	
1.3	Each processor must have at least 8 cores. The server must have a total of at least 16 cores.	<i>Her bir işlemci en az 8 çekirdekli olmalıdır. Sunucuda toplam olarak en az 16 çekirdek olmalıdır.</i>	
1.4	Each processor must have at least 11 MB of cache.	<i>Her bir işlemci üzerinde en az 11 MB önbellek bulunmalıdır.</i>	
1.5	Each processor must have at least 2 UPI (Ultra Path Interconnect) connections.	<i>Her bir işlemci en az 2 adet UPI (Ultra Path Interconnect) bağlantı sayısına sahip olmalıdır.</i>	
1.6	Each memory used on the server will be PC4, DDR4.	<i>Sunucu üzerinde kullanılan her bir bellek PC4, DDR4 olacaktır.</i>	
1.7	There will be at least 384 GB of memory on the server. (each 2666MT/s and at least a capacity of 12*32 GB).	<i>Sunucu üzerinde her biri 2666MT/s, en az 12 adet 32 GB kapasitesinde olan, toplamda en az 384 GB bellek bulunacaktır.</i>	
1.8	There will be at least 24 memory slots on the server.	<i>Sunucu üzerinde en az 24 adet bellek yuvası bulunacaktır</i>	
1.9	Memory modules will be ECC(Error Check Correction).	<i>Bellek modülleri ECC(Error Check Correction) özelliğinde olacaktır.</i>	
1.10	There should be a built-in dual SD card module on the server to be proposed.	<i>Teklif edilecek sunucu üzerinde dahili çift SD kart takılabilen modül bulunmalıdır</i>	
1.11	The server must have at least 2 microSDHC/SDXC cards with a capacity of 64 GB provided by the server manufacturer.	<i>Sunucu için en az 2 adet, sunucu üreticisinin sağladığı 64 GB kapasiteli, microSDHC/SDXC kart bulunmalıdır</i>	
1.12	Each server must have at least 1 interface to provide remote access and management at 10/100/1000Mbps.	<i>Her bir sunucu üzerinde en az 1 adet 10/100/1000Mbps hızında uzaktan erişim ve yönetim sağlayacak arabirimi olmalıdır.</i>	
1.13	Each server must have at least 4 1Gb Base-T and 2 10GB SFP+ Ethernet ports	<i>Her bir sunucu üzerinde en az 4 adet 1Gb Base-T ve 2 adet 10GB SFP+ ethernet bağlantı noktası bulunmalıdır</i>	
1.14	At least 2 SR SFP+ modules must be supplied with each server. SFP+ modules must be the original product. Equivalent products will not be accepted.	<i>Her bir sunucu ile birlikte en az 2 adet SR SFP+ modül verilmelidir. SFP+ modüller orijinal ürün olmalıdır. Muadil ürünler kabul edilmeyecektir</i>	
1.15	Each server must have at least	<i>Her bir sunucu üzerinde en az</i>	

	2 external HBA controllers running as 12Gbps SAS.	<i>2 adet 12Gbps SAS olarak çalışan harici HBA kontrol birimi bulunmalıdır.</i>	
1.16	The PDU and cables required for the server will be delivered together without previous use.	<i>Sunucu için gerekli PDU ve kablolar birlikte daha önce kullanılmamış olarak teslim edilecektir.</i>	
1.17	Each server must have at least 2 redundant power supplies, each with a power of 750W, which can be disassembled and installed during operation. At least 2 redundant power supplies, each with 2400W power, should be installed on the server if necessary.	<i>Her bir sunucu üzerinde çalışma esnasında sökülüp takılabilen; en az 2 adet, her biri 750W gücünde yedekli güç kaynağı bulunmalıdır. Sunucu üzerine gerektiğinde en az 2 adet, her biri 2400W gücünde yedekli güç kaynağı takılabilmelidir.</i>	
1.18	For each server, fans must be installed with at least 6 redundant and all fan slots of the proposed system that can be disassembled and installed during operation.	<i>Her bir sunucu için, çalışma esnasında sökülüp takılabilen en az 6 adet yedekli ve teklif edilen sistemin tüm fan yuvaları dolu olacak şekilde fanlar takılı bulunmalıdır.</i>	
1.19	The server must support Trusted Platform Module 2.0 (TPM 2.0) and be offered with the necessary licenses	<i>Sunucuda Trusted Platform Module 2.0 (TPM 2.0) desteği bulunmalı ve gerekli lisanslar ile teklif edilmelidir</i>	
1.20	There must be at least 1 VGA port and 4 USB ports on the server to be offered.	<i>Teklif edilecek sunucu üzerinde en az 1 adet VGA portu, toplam 4 adet USB portu bulunmalıdır.</i>	
1.21	There must be at least 1 PCIe Gen3 x16 at least 4 PCIe slots on the server to be offered.	<i>Teklif edilecek sunucu üzerinde en az 1 adedi PCIe Gen3 x16 en az 4 adet PCIe slotu bulunmalıdır.</i>	
1.22	Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi operating systems may be installed on the servers.	<i>Sunucular üzerine, Canonical Ubuntu LTS, Citrix XenServer, Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi işletim sistemleri kurulabilecektir.</i>	
1.23	The server to be offered must have a graphics card with at least 16mb of memory and supports a resolution of at least 1920*1200.	<i>Teklif edilecek sunucu üzerinde embedded olarak en az 16mb belleğe sahip ve en az 1920*1200 çözünürlüğü destekleyen grafik kartı bulunmalıdır.</i>	
1.24	At least 6 Single wide or at	<i>Teklif edilecek sunucu üzerine</i>	

	least 3 Double wide GPU cards can be installed on the server to be offered in necessary cases.	<i>gerektiğinde en az 6 adet Single wide veya gerektiğinde en az 3 adet Double wide GPU kart takılabilmelidir</i>	
1.25	The server must have a lockable front cover to prevent physical interference.	<i>Sunucu üzerinde fiziksel müdahaleleri engelleyebilmek için kilitlenebilir ön kapak bulunmalıdır.</i>	
1.26	The files required for system installation on the proposed server must be embedded and the system must be installed through the embedded system without the need for any disk drive.	<i>Teklif edilen sunucu üzerinde sistem kurulumu için gerekli dosyalar embedded olmalıdır ve herhangi bir disk, sürücü ye ihtiyaç olmadan embedded sistem üzerinden sistem kurulabilmelidir.</i>	
1.27	The server must have an LCD screen or warning lights showing system name, serial number, remote management IP number, power consumption, and fault information that ensures easy detection of failures.	<i>Sunucu üzerinde sistem ismi, seri numarası, uzaktan yönetim IP numarası, güç tüketimi ve arızaların kolay tespit edilebilmesini sağlayan arıza bilgilerini gösteren LCD ekran ya da uyarı ışıkları bulunmalıdır.</i>	
1.28	The server must have a remote management module with its own 1 Gb physical port that will provide access with HTTPS and SSLv2 certificates.	<i>Sunucu üzerinde HTTPS ve SSLv2 sertifika ile erişim sağlayacak kendine ait 1 Gb hızında fiziksel bağlantı noktasına sahip uzaktan yönetim modülü bulunmalıdır.</i>	
1.29	One of the USB ports on the front panel of the server must be accessible by the remote management port, a firmware update or authorization can be made with the USB memory that can be installed through this port when the server is closed, and the remote management web interface must be accessed by connecting it to a computer by USB cable when the remote management network is not installed or working.	<i>Sunucu ön panelinde bulunan USB portlardan bir adeti uzaktan yönetim portu tarafından erişilebilmeli, sunucu kapalı olduğu esnada bu port üzerinden takılabilecek USB bellek ile firmware güncellemesi veya provizyonlama yapılabilmeli ve uzaktan yönetim networkünün kurulu olmadığı veya çalışmadığı esnada USB kablo ile bir bilgisayara bağlayarak uzaktan yönetim web ara yüzüne erişilebilmelidir.</i>	
1.30	The remote management module must have HTML5 support and modern web	<i>Uzaktan yönetim modülünün HTML5 desteği olmalı ve herhangi ajan, eklenti</i>	

	servers should be managed without installing any agents, plugins, remote KVM access should be made, the operating system should be established by remote media connection and updates should be made.	<i>yüklenmeden modern web sunucuları yönetilmeli, uzaktan KVM erişimi yapılabilirmeli, uzaktan medya bağlantısı yapılarak işletim sistemi kurulabilmeli ve güncellemeler yapılabilirmelidir.</i>	
1.31	Servers must support virtual media, use USB sticks, CDs, DVDs, etc. connected to a remote computer.	<i>Sunucular sanal medya özelliğini desteklemelidir, uzaktaki bir bilgisayara bağlı USB bellek, CD, DVD, vb. medyaları kullanabilmelidir.</i>	
1.32	The remote management module should be able to manage the server RAID card, configure the disks to be added to the server later, and increase its capacity by adding disks to existing RAID groups.	<i>Uzaktan yönetim modülü sunucu RAID kartının yönetimini gerçekleştirebilmeli, sunucuya sonradan eklenecek disklerin RAID yapılandırmasını yapabilmeli ve mevcut RAID gruplarına disk eklemesi yaparak kapasitesini artırılmasını sağlayabilmelidir.</i>	
1.33	The server must be able to check the security and authenticity of the BIOS, firmware etc. files to be installed on it through the certificate, and there must be a secure non-volatile memory space on the server that ensures that security certificates are protected against attacks.	<i>Sunucu, üzerine yüklenecek BIOS, firmware vb dosyalarının sertifika vasıtası ile güvenliğini ve orijinalliğini kontrol edebilmeli, sunucu üzerinde, güvenlik sertifikalarının saldırılara karşı korunmasını sağlayan, uçucu olmayan güvenli bir bellek alanı bulunmalıdır.</i>	
1.34	There should be a metal alloy sliding rail system with accessories to prevent the proposed server from bending when pressed to ensure that it is pulled forward from the cab during operation.	<i>Teklif edilecek sunucunun çalışma esnasında kabinde öne çekilerek müdahale edilmesini sağlayacak üzerine baskı olduğunda eğilmesini engelleyecek aksesuarlara sahip metal alaşımlı kayan ray sistemi bulunmalıdır.</i>	
1.35	The server to be offered must have access and management support via mobile phone or tablet upon request.	<i>Teklif edilecek sunucunun istenildiğinde cep telefonu veya tablet üzerinden erişim ve yönetim desteği olmalıdır.</i>	
1.36	All components supplied with	<i>Sunucu beraber verilen bütün</i>	

	the server must be manufactured by the server manufacturer or approved by the server manufacturer and supplied by the server manufacturer and the current configuration of the server must be questioned through a portal belonging to the manufacturer, the server guarantee must cover all components on the server.	<i>komponentler sunucu üreticisi tarafından üretilmiş veya sunucu üreticisi tarafından onaylanarak tedariki sunucu üreticisi tarafından yapılmış olmalı ve üreticiye ait bir portal üzerinden sunucunun güncel konfigürasyonu sorgulanabilmeli, sunucu garantisi, sunucu üzerinde gelen bütün komponentleri kapsamalıdır.</i>	
1.37	It will operate on the city grid with 220 V AC and 50 Hz single or three-phase energy supply. Feed cable plugs for energy input will be of the appropriate type to the power distribution units in the existing cabinets.	<i>220 V AC ve 50 Hz tek veya üç faz enerji beslemesi ile şehir şebekesinde çalışacaktır. Enerji girişi için besleme kablo fişleri mevcut kabinler içerisindeki güç dağıtım ünitelerine uygun tipte olacaktır.</i>	
1.38	Servers will have a manufacturer's warranty on the next business day for at least 3 years. The letter that the warranty is given by the manufacturer should be provided in delivery time.	<i>Sunucular en az 3 yıl boyunca ertesi iş günü üretici garantisine sahip olacaktır. Garantinin üretici firma tarafından verildiğine dair yazı teslimat sırasında ibraz edilecektir.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
2. Data Storage Unit		<i>Veri Depolama ünitesi</i>	Brand/Model // Marka/Model:
2.1	The data storage manufacturer to be offered will be the same brand or a brand of a solution partner as the proposed server computers.	<i>Teklif edilecek veri depolama üreticisi, teklif edilen sunucu bilgisayarlar ile aynı marka ya da çözüm ortağı firmanın markası olacaktır.</i>	
2.2	The external data storage system to be proposed must not consist of combining multiple data storage	<i>Teklif edilecek harici veri depolama sistemi, birden fazla veri depolama sisteminin kümeleme veya benzeri</i>	

	systems with clustering or similar methods.	<i>yöntemlerle birleştirilmesinden oluşmuş olmamalıdır.</i>	
2.3	Measures must be taken against a single-point error in the external data storage system to be offered and ensure that the backup unit data storage system operates continuously in case of failure of any part.	<i>Teklif edilecek harici veri depolama sisteminde tek noktadan hata durumuna karşı önlemler alınmış olmalı ve herhangi bir parçanın arızasında yedek birim veri depolama sisteminin durmadan çalışmasını sağlamalıdır.</i>	
2.4	In case of any failure in the external data storage system to be proposed, the replacement of any part in the system (disc, power supply, fans, etc.) should be carried out without requiring system shutdown.	<i>Teklif edilecek harici veri depolama sisteminde herhangi bir sorun çıkması durumunda sistem içerisindeki herhangi bir parçanın (disk, güç kaynağı, fanlar, vs.) değiştirilmesi sistem herhangi bir sistem kapanması gerektirmeden yapılabilmelidir.</i>	
2.5	There must be two control units (dual controllers) on the external storage system.	<i>Harici depolama sistemi üzerinde iki adet kontrol ünitesi (dual controller) bulunmalıdır.</i>	
2.6	The proposed data storage unit must be able to connect the server with 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI, and 12 Gb SAS ports. At least 8 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI, and 12 Gb SAS ports should be installed on the proposed data storage unit as needed. In addition, the data storage unit must support at least 4 16Gb FC and at least 4 10Gb SFP+ ports on the device at the same time if desired (multi-protocol ports).	<i>Teklif edilen veri depolama ünitesi, 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI ve 12 Gb SAS portları ile sunucu bağlantısını sağlayabilmelidir. Teklif edilen veri depolama ünitesi üzerine ihtiyaca göre en az 8 adet 16 Gb FC, 10 Gb SFP+ iSCSI, 10 Gb Base-T iSCSI ve 12 Gb SAS portları takılabilmelidir. Ayrıca veri depolama ünitesi istenirse en az 4 adet 16Gb FC ve en az 4 adet 10Gb SFP+ portun aynı anda cihaz üzerinde bulunmasını desteklemelidir (multi-protocol ports).</i>	
2.7	Each controller will have a total of at least 8 pieces of 12 Gbps SAS ports, including at least 4 SAS ports at a speed of 12 Gbps.	<i>Her kontrol ünitesi (controller) üzerinde 12 Gbps hızında en az 4 adet SAS port olmak üzere toplamda en az 8 adet 12 Gbps SAS port</i>	

		<i>bulunacaktır.</i>	
2.8	At least 2 pieces, at least 2 meters long, 12 Gbps, HD Mini-SAS to HD Mini-SAS cable will be supplied with the storage unit. All cables must belong to the storage manufacturer.	<i>Depolama ünitesi ile birlikte en az 2 adet, en az 2 metre uzunluğunda, 12 Gbps, HD Mini-SAS to HD Mini-SAS kablo verilecektir. Tüm kablolar depolama üreticisine ait olmalıdır.</i>	
2.9	Each control unit must have a management port with a speed of at least 1Gbps.	<i>Her kontrol ünitesi yönetim için en az 1Gbps hızına sahip yönetim portu bulunmalıdır.</i>	
2.10	Each controller on the external disk unit to be offered must have at least 8 GB of memory and a total of 16 GB of memory. This capacity must be dram type. Within the scope of this cache capacity, fields created with SSD/FMD, I/O card will not be accepted.	<i>Teklif edilecek harici disk ünitesi üzerinde bulunan her kontrol ünitesi üzerinde en az 8, toplamda ise 16 GB bellek bulunmalıdır. Bu kapasite DRAM tipinde olmalıdır. Bu ön bellek kapasitesi kapsamında SSD/FMD, I/O kart ile oluşturulan alanlar kabul edilmeyecektir.</i>	
2.11	Firmware updates should be available without causing disruption to the running system.	<i>Çalışan sistem üzerinde kesinti yaratmadan firmware güncellemeleri yapılabilmelidir.</i>	
2.12	The Storage Unit should be able to expand to at least 276 disk capacity with the proposed controllers and grow to at least 3PB capacity.	<i>Depolama Ünitesi, teklif edilen kontrol birimleri ile en az 276 adet disk kapasitesine genişleyebilmeli ve en az 3PB kapasitesine kadar büyüebilmelidir.</i>	
2.13	The system disk boost should be incremental in the form of racks and these racks should be manageable with an integrated HTML5 web-based GUI interface. Racks should be able to be created from 24 2.5" disks to provide the total number of discs, and the connection between the racks should be made with a 12 Gbit SAS interface. Each of the shelves should be no more than 2U high.	<i>Sistem disk artırımı raflar şeklinde arttırılabilir olmalı ve bu raflar entegre bir HTML5 web tabanlı GUI arayüzü ile yönetilebilir olmalıdır. Raflar toplam disk sayısını sağlamak üzere 24 adet 2.5" disklerden oluşturulabilmeli ve raflar arasındaki bağlantı 12 Gbit hızında SAS arayüz ile yapılmalıdır. Rafların her biri en fazla 2U yükseklikte olmalıdır.</i>	
2.14	The system must have at least 12 SSD drives with a connection speed of 12Gbps,	<i>Sistem üzerinde en az 12 adet, 12Gbps bağlantı hızında, 960 GB kapasiteli SSD</i>	

	ssd technology with a capacity of 960 GB, and SAS disks with a capacity of 1.8 TB with a rotational speed of at least 12 10000 RPM.	<i>teknolojisinde diskler ve en az 12 adet 10000 RPM dönüş hızında, 1.8 TB kapasiteli SAS diskler bulunmalıdır.</i>	
2.15	The disks used must be high-performance SAS, NL-SAS, SSD, and FIPS certified self-encrypting SAS and SSD in accordance with the selected disc racks.	<i>Kullanılan diskler seçilen disk raflarına uygun şekilde yüksek performanslı SAS, NL-SAS, SSD ve FIPS sertifikalı self-encrypting SAS ve SSD olabilmelidir.</i>	
2.16	The proposed data storage system must monitor the I/O that each disk makes, proactively monitor the health status performance graph, and work to provide the necessary warnings before the disk fails. Systems that fail to provide this must offer 30% additional capacity.	<i>Teklif edilen veri depolama sistemi her disk in yaptığı I/O yu izlemeli sağlık durumunu performans grafiğini proaktif olarak izlemeli ve disk bozulmadan önce gerekli uyarıları verecek şekilde çalışmalıdır. Bunu sağlayamayan sistemler %30 ilave kapasite verecek şekilde teklif etmelidirler.</i>	
2.17	The system must have Distributed RAID or similar technology that reduces rebuild times when disk failures occur on it.	<i>Sistem, üzerinde disk arızaları meydana geldiği zaman, yeniden oluşturma sürelerini azaltan Distributed RAID veya benzeri bir teknolojiye sahip olmalıdır.</i>	
2.18	The system should be able to support at least 64 host connections with a fiber connection option.	<i>Sistem Fiber bağlantı seçeneği ile en az 64 adet host bağlantısını destekleyebilmelidir.</i>	
2.19	The external disk system must support RAID levels 0, 1, 5, 6, and 10. Alternative data protection methods will not be accepted.	<i>Harici disk sistemi 0, 1, 5, 6 ve 10 RAID seviyelerini desteklemelidir. Alternatif veri koruma yöntemleri kabul edilmeyecektir.</i>	
2.20	Additions should be made to the virtual disk groups being used in the system without interruption of access.	<i>Sistemde kullanılmakta olan sanal disk gruplarına erişim kesintisi olmadan ilaveler yapılabilmelidir.</i>	
2.21	All licenses supported by the data storage unit (snapshot, clone, read cache, auto-tiering, replication, etc.) must be offered together with the proposed data storage unit in order to avoid	<i>Teklif edilen veri depolama ünitesi ile birlikte ileri tarihlerde ek maliyet olmaması açısından, veri depolama ünitesinin desteklediği tüm lisanslar (snapshot, clone, read cache,</i>	

	additional costs at a later date.	<i>auto tiering, replikasyon vb.) ile birlikte teklif edilmelidir.</i>	
2.22	The proposed data storage system should support the use of SSDs, which can be added to the system if desired, as a read-cache. SSD cache capacity can be raised up to 4TB. If there is an additional license requirement for this feature, it must be included in the offer.	<i>Teklif edilecek veri depolama sistemi, istendiği takdirde sisteme eklenebilecek SSD'lerin okuma ve yazma amaçlı önbellek olarak kullanımını desteklemelidir. SSD önbellek kapasitesi 4TB'a kadar yükseltilebilmelidir. Bu özellik için ek bir lisans gereksinimi varsa teklife dahil edilmelidir.</i>	
2.23	The data storage system to be offered must have automatic data tiering that supports at least 3 layers (SSD, SAS, NL-SAS/SATA). By monitoring data activities on storage areas at the sub-LUN level, the data storage system should be able to automatically move heavily used sub-logical areas to faster storage and underused sub-logical areas to slower storage (automatic data tiering). Within the scope of this property, the data must be in the form of moving movements between layers, not in the form of copying. If a license is required to provide such a feature, the required licenses will be included in the offer for the maximum capacity supported by the system.	<i>Teklif edilecek veri depolama sistemi, en az 3 katmanı (SSD, SAS, NL-SAS/SATA) destekleyen otomatik veri katmanlandırma özelliğine sahip olmalıdır. Veri depolama sistemi, depolama alanları üzerindeki veri aktivitelerini alt mantıksal alan (sub-LUN – blok) seviyesinde izleyerek, yoğun kullanılan alt mantıksal alanları daha hızlı depolama alanına ve az kullanılan alt mantıksal alanları daha yavaş depolama alanına otomatik olarak taşıyabilmelidir (otomatik veri katmanlandırma). Bu özellik kapsamında verilerin katmanlar arasındaki hareketleri taşıma şeklinde olmalı, kopyalama şeklinde olmamalıdır. Söz konusu özelliğin sağlanabilmesi için lisans gerekmesi durumunda, gerekli olan lisanslar, sistemin desteklediği maksimum kapasite için teklife dahil edilecektir.</i>	
2.24	The proposed data storage unit must support "thin provisioning".	<i>Teklif edilen veri depolama ünitesi "thin provisioning" desteği olmalıdır.</i>	
2.25	At least 512 (five hundredonics) LUNs must be created in the proposed data	<i>Teklif edilen veri depolama ünitesinde en az 512 (beşyüzoniki) LUN</i>	

	storage unit.	<i>yaratılabilmelidir.</i>	
2.26	The external data storage system to be offered must be able to receive snapshots and full copies (clones) and return them (restored). The licenses required for this feature will be added to the offer for the maximum capacity supported by the system.	<i>Teklif edilecek harici veri depolama sistemi snapshot (anlık kopya) ve tam kopya (clone) alabilmeli ve bu kopyalardan geri dönebilmelidir (restore). Bu özellik için gerekli lisanslar sistemin desteklediği maksimum kapasite için teklife eklenecektir.</i>	
2.27	The external data storage system to be offered should use the ROW (Redirect on Write) method and not the COW (Copy on Write) method to avoid affecting the snapshot. Working principles will be documented with manufacturer's documents.	<i>Teklif edilecek harici veri depolama sistemi anlık kopyalama (snapshot) performansın etkilenmemesi için ROW (Redirect on Write) metodunu kullanmalı, COW (Copy on Write) metodunu kullanmamalıdır. Çalışma prensipleri üretici dökümanları ile belgelenecektir.</i>	
2.28	The proposed data storage unit must support at least 1024 snapshots.	<i>Teklif edilen veri depolama ünitesinin en az 1024 adet snapshot desteği olmalıdır.</i>	
2.29	The external data storage system to be offered is asynchronous, it must support replication. If additional hardware and licenses are required for this feature, it must be added to the offer for maximum capacity.	<i>Teklif edilecek harici veri depolama sistemi asenkron, replikasyonu desteklemelidir. Bu özellik için ek donanım ve lisans gerekiyorsa teklife maksimum kapasite için eklenmelidir.</i>	
2.30	The proposed data storage unit must have at least 2 redundant power supply with a power of at least 580 Watts. 2 power cables must be supplied with the data storage unit.	<i>Teklif edilen veri depolama ünitesi en az 2 adet, en az 580 Watt gücünde yedekli güç kaynağına (redundant power supply) sahip olmalıdır. Veri depolama ünitesi ile birlikte 2 adet güç kablosu verilmelidir.</i>	
2.31	External disk unit must support at least VMware 6.0, 6.5, and 6.7; Windows Server 2012, 2016,2019, RHEL 6.0, and 7.4 SLES 12.3 operating systems.	<i>Harici disk ünitesi en az VMware 6.0, 6.5 ve 6.7; Windows Server 2012, 2016,2019, RHEL 6.0 ve7.4, SLES 12.3 işletim sistemlerini desteklemelidir.</i>	
2.32	The external disk volume must support VMware	<i>Harici disk ünitesinin VMware vSphere (ESXi), Microsoft</i>	

	vSphere (ESXi), Microsoft Hyper-V, and vCenter SRM.	<i>Hyper-V ve vCenter SRM desteği olmalıdır.</i>	
2.33	Data Storage system management should be web-based without the need to install additional software.	<i>Veri Depolama sisteminin yönetimi ek bir yazılım yüklemeye gerek kalmadan web tabanlı olarak yapılabilmelidir.</i>	
2.34	The external data storage system to be offered will have the ability to alert the system administrator by e-mail in case of a failure on it.	<i>Teklif edilecek harici veri depolama sistemi, üzerinde oluşan bir arıza durumunda sistem yöneticisini e-posta ile uyarma özelliğine sahip olacaktır.</i>	
2.35	The data storage unit should have a next-day guarantee of the manufacturer for at least 3 years.	<i>Veri depolama ünitesi en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
3. Virtualization Software		<i>Sanallaştırma Yazılımı</i>	Brand/Model // <i>Marka/Model:</i>
3.1.	Virtualization software will be licensed for a total of 6 CPUs.	<i>Sanallaştırma yazılımı toplam 6 CPU için lisanslandırılacaktır.</i>	
3.2.	The proposed virtualization software must allow over-commitment of virtual machines to be created on the same physical server above existing system resources.	<i>Teklif edilen sanallaştırma yazılımı aynı fiziksel sunucu üzerinde oluşturulacak sanal makinelerin mevcut sistem kaynaklarının üzerinde kaynak atanmasına (over-commitment) izin vermelidir.</i>	
3.3.	The proposed virtualization software must support SMP (Symetric Multi Processing). In the proposed system, 128 virtual CPUs should be assigned to each virtual machine at any time.	<i>Teklif edilen sanallaştırma yazılımı SMP (Symetric Multi Processing) desteği olmalıdır. Teklif edilen sistemde her bir sanal makinaya istenildiğinde 128 adet sanal CPU atanabilmelidir.</i>	
3.4.	With the proposed virtualization software, 1TB of virtual memory should be	<i>Teklif edilen sanallaştırma yazılımı ile her bir sanal makinaya 1TB sanal bellek</i>	

	assigned to each virtual machine.	<i>atanabilmelidir.</i>	
3.5.	The proposed virtualization software should be able to enlarge the virtual machine disk as it fills up, instead of retrieving the assigned disk space for each virtual machine directly from the disk pool. (Thin Provisioning)	<i>Teklif edilen sanallaştırma yazılımı gerektiğinde her bir sanal makine için atanan disk alanın doğrudan disk havuzundan almak yerine, sanal makine diski doldukça büyütebilmelidir. (Thin Provisioning)</i>	
3.6.	The proposed virtualization software guest operating system "GuestOS" must support current versions of Windows 8, Windows 10, Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, SUSE Linux, Debian, Oracle Linux, MacOSX, FreeBSD operating systems.	<i>Teklif edilen sanallaştırma yazılımı misafir işletim sistemi "Guest OS" olarak, Windows 8, Windows 10 , Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Centos, Redhat, Ubuntu, Solaris, SUSE Linux, Debian, Oracle Linux , MacOSX, FreeBSD işletim sistemlerinin güncel versiyonlarını desteklemelidir.</i>	
3.7.	The proposed virtualization software must allow the file system containing the disks and virtual machines given to virtual machines to be enlarged while the system is running.	<i>Teklif edilen sanallaştırma yazılımı, sanal makinalara verilen disklerin ve sanal makinaların bulunduğu dosya sisteminin sistem çalışırken büyütülmesine izin vermelidir.</i>	
3.8.	The proposed virtualization software should enable the assignment of 62TB virtual disks to virtual machines.	<i>Teklif edilen sanallaştırma yazılımı sanal makinalara 62TB boyutunda sanal diskler atanmasına olanak sağlamalıdır.</i>	
3.9.	Proposed virtualization software must be able to manage 64TB of storage	<i>Teklif edilen sanallaştırma yazılımı 64TB boyutundaki depolama alanlarını yönetebilmelidir</i>	
3.10.	Support data storage technologies such as FC, iSCSI, and NFS and data storage units that work with these technologies with the proposed virtualization software.	<i>Teklif edilen sanallaştırma yazılımı ile FC, iSCSI ve NFS gibi veri depolama teknolojilerini ve bu teknolojilerle çalışan veri depolama ünitelerini desteklemelidir.</i>	
3.11.	With the proposed virtualization software, authorization should be	<i>Teklif edilen sanallaştırma yazılımı ile sistemde yetkilendirme yapılabilmeli,</i>	

	made in the system, allowing certain operational persons to access the entire virtual system or part of the virtual system and carry out management operations.	<i>belirli operasyonel kişilerin tüm sanal sisteme veya sanal sistemin bir kısmına erişmelerine ve yönetim operasyonlarını gerçekleştirebilmelerine imkan tanımalıdır.</i>	
3.12.	With the proposed virtualization software, system performance should be monitored instantly or retrospectively for parameters such as CPU, memory, disk, and network, and a report should be obtained.	<i>Teklif edilen sanallaştırma yazılımı ile sistem performansı CPU, memory, disk ve network gibi parametreler için anlık veya geçmişe doğru izlenebilmeli, rapor alınabilmelidir.</i>	
3.13.	The proposed virtualization software must include centralized management software that enables the management of all virtual servers from a single center. The management software will be the full version. (Will be offered with centralized management software licenses)	<i>Teklif edilen sanallaştırma yazılımı tüm sanal sunucuların tek bir merkezden yönetimini sağlayan merkezi yönetim yazılımını içermelidir. Yönetim yazılımı tam sürüm olacaktır. (Merkezi yönetim yazılımı lisansları ile teklif edilecektir)</i>	
3.14.	The centralized management software that comes with the proposed virtualization software must be connected and managed from the web interface.	<i>Teklif edilen sanallaştırma yazılımı ile gelen merkezi yönetim yazılımı web arayüzünden bağlanıp yönetmeye olanak sağlamalıdır.</i>	
3.15.	The proposed virtualization software must allow VLAN assignment to virtual servers.	<i>Teklif edilen sanallaştırma yazılımı sanal sunuculara VLAN atanmasına izin vermelidir.</i>	
3.16.	The proposed virtualization software must allow a copy of the virtual servers to be made while they are open.	<i>Teklif edilen sanallaştırma yazılımı sanal sunucuların açıkken bir kopyasının çıkarılmasına izin vermelidir.</i>	
3.17.	The proposed virtualization software should be able to transfer running virtual machines to another server within the virtualization system without the need for shared disk space when	<i>Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makinaları ihtiyaç duyulduğunda paylaşımlı bir disk alanına ihtiyaç duymaksızın sanallaştırma sistemi içindeki başka bir</i>	

	needed and perform this process for multiple virtual machines at the same time.	<i>sunucuya aktarabilmeli, bu işlemi aynı anda birden fazla sanal makina için gerçekleştirebilmelidir.</i>	
3.18.	There should be clustering service support in the form of automatic operation of virtual machines that shut down when there is an out-of-control stop on one of the servers defined in the proposed virtualization software. This service should be prioritized between virtual machines.	<i>Teklif edilen sanallaştırma yazılımı içerisinde tanımlı sunuculardan birisinde kontrol dışı bir durma olduğunda kapanan sanal makinelerin sistemdeki diğer sunucular tarafından otomatik olarak çalıştırılması şeklinde kümeleme hizmeti desteği olmalıdır. Bu hizmet için sanal makineler arasında önceliklendirme yapılabilmelidir.</i>	
3.19.	The proposed virtualization software must include a module that takes backups of Windows and Linux virtual machines running into the disk environment. This module should be able to store backed-up data by singularization.	<i>Teklif edilen sanallaştırma yazılımı içerisinde çalışan Windows ve Linux sanal makinelerin yedeklerini disk ortamına alan bir modülü bulunmalıdır. Bu modül yedeklenmiş verileri tekilleştirme yaparak saklayabilmelidir.</i>	
3.20.	The proposed virtualization software should allow designated virtual machines to replicate on virtualization servers in the same location or remote location.	<i>Teklif edilen sanallaştırma yazılımı belirlenen sanal makinelerin aynı lokasyondaki veya uzak bir lokasyondaki sanallaştırma sunucuları üzerine replikasyon yapmasına olanak tanımalıdır.</i>	
3.21.	The proposed virtualization software should be able to work integrated with third-party antivirus solutions and enable virus scanning on virtual machines using agency-independent architecture.	<i>Teklif edilen sanallaştırma yazılımı üçüncü parti antivirus çözümleri ile entegre çalışabilmeli ve ajansız mimari kullanarak sanal makineler üzerinde virüs taraması yapılmasına olanak sağlamalıdır.</i>	
3.22.	The proposed virtualization software must be able to move working virtual machines between their disks and storage areas.	<i>Teklif edilen sanallaştırma yazılımı çalışır durumdaki sanal makineleri diskleri ile birlikte depolama alanları arasında taşıyabilmelidir.</i>	
3.23.	The proposed virtualization software must support the	<i>Teklif edilen sanallaştırma yazılımı çalışır durumdaki</i>	

	addition of CPU, memory, disk, and network cards to running virtual machines.	<i>sanal makinalara CPU, memory, disk ve network kartı eklenmesini desteklemelidir.</i>	
3.24.	The proposed virtualization software should be able to ensure that the physical servers it operates for the selected virtual machines continue to operate from other physical servers without interruption in the event of an unplanned outage.	<i>Teklif edilen sanallaştırma yazılımı seçilen sanal makinalar için çalıştığı fiziksel sunucuların plansız bir kesinti yaşaması durumunda, kesintisiz olarak diğer fiziksel sunuculardan çalışmasına devam etmesini sağlayabilmelidir.</i>	
3.25.	Performance monitoring software should be able to monitor performance according to disk, memory, CPU, and network resources.	<i>Performans izleme yazılımı disk, bellek, cpu ve network kaynaklarına göre performans izlemesi yapabilmelidir.</i>	
3.26.	Performance monitoring software should be able to automatically make adaptive threshold definitions for resource usage by learning the system resource usage curve and be able to sound the alarm when resource usage rises below or above this lower threshold.	<i>Performans izleme yazılımı sistem kaynak kullanım eğrisini öğrenerek otomatik olarak kaynak kullanımı için adaptif eşik tanımlamaları yapabilmeli ve kaynak kullanımını bu alt eşiğin altına veya üst eşiğin üstüne çıktığında alarm verebilmelidir.</i>	
3.27.	Performance monitoring software should be able to detect incidents that may cause performance problems by associating alarms, errors, or warnings in the system with source usage graphs when necessary.	<i>Performans izleme yazılımı gerektiğinde sistemdeki alarm, hata veya uyarıları kaynak kullanım grafikleri ile ilişkilendirerek performans sorununa neden olabilecek olayları tespit edebilmelidir.</i>	
3.28.	Performance monitoring software must have its own database, not need a third-party database.	<i>Performans izleme yazılımı kendi veritabanına sahip olmalı, üçüncü parti bir veritabanına ihtiyaç duymamalıdır.</i>	
3.29.	Performance monitoring software should be able to monitor all virtual machines in the system to check whether the amounts of resources assigned to virtual machines are correct and to	<i>Performans izleme yazılımı sistemdeki tüm sanal makinaları izleyerek sanal makinalara atanan kaynak miktarlarının doğru olup olmadığını kontrol edebilmeli, bu konuda iyileştirmeler</i>	

	make improvements in this regard.	yapabilmek için tavsiyelerde bulunabilmelidir.	
3.30.	All software updates and security patches that will be issued for at least 3 years with licenses for the proposed solution must be installed, as well as 5 days and 9 hours of support for 3 years.	Teklif edilen çözüme ait lisanslar ile birlikte en az 3 yıl boyunca çıkacak tüm yazılım güncellemeleri ve güvenlik yamaları yüklenebilmelidir, ayrıca 3 yıl boyunca 5 gün 9 saat destek hizmeti verilmelidir.	
Item to be supplied description		Tedarik edilecek ürün tanımı	Offered technical specifications by the Bidder shall be inserted in English Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir
4. Backup Software		Yedekleme Yazılımı	Brand/Model // Marka/Model:
4.1.	The software must be able to back up virtual machines running on the Microsoft Hyper-V and VMware vSphere virtualization platform to the application-consistent image-based disk.	Yazılım Microsoft Hyper-V ve VMware vSphere sanallaştırma platformunda çalışan sanal makinelerin uygulama tutarlı imaj tabanlı diske yedeklemesini yapabilmelidir.	
4.2.	The software's management console must be able to work on any physical or virtual, server, or personal computer with a 64-bit Microsoft Windows operating system.	Yazılımın yönetim konsolu 64 bit bir Microsoft Windows işletim sistemine sahip herhangi bir fiziksel veya sanal, sunucu veya kişisel bilgisayar üzerinde çalışabilmelidir.	
4.3.	The software must be licensed on the basis of the physical processor of the main servers running the virtual machines that are protected (backed up and/or replicated). There should be no licensing model based on the number of Virtual Machines, disk capacities,	Yazılımın lisanslaması korunmakta (yedeklenmekte ve/veya replike edilmekte) olan sanal makineleri çalıştıran ana sunucuların fiziksel işlemcisi bazında olmalıdır. Sanal Makina sayısı, disk kapasiteleri ve uygulama ajanlarına göre bir lisanslama modeli olmamalıdır.	

	and application agents.		
4.4.	In order to improve the backup and replication performance of the Software, the number of structural components such as consoles, proxics, and storage areas should be increased without the need for an additional license.	<i>Yazılımın yedekleme ve replikasyon performansını arttırmak amacı ile konsol, proksi ve depolama alanları gibi yapısal bileşenlerinin sayısı ilave bir lisans gerektirmeden arttırılabilmelidir.</i>	
4.5.	The Software must be able to use Windows, Linux, CIFS/SMB file shares, and devices that offer singularization to store backed-up virtual machines.	<i>Yazılım, yedeklenen sanal makinaları saklamak için Windows, Linux, CIFS/SMB dosya paylaşımlarını ve tekilleştirme sunan cihazları kullanabilmelidir.</i>	
4.6.	The software must use the Changing Block Tracking (CBT) feature offered by hypervisors for incremental backups.	<i>Yazılım artımlı yedekler için hipervizörlerin sunduğu Değişen Blok Takibi (CBT) özelliğini kullanmalıdır.</i>	
4.7.	The Software must provide backup options over the Direct Data Storage network, over the Network, or through the Hypervisor I/O platform when reading backups from the source.	<i>Yazılım yedekleri kaynaktan okurken Doğrudan Veri Depolama ağı üzerinden, Ağ üzerinden veya Hipervizör I/O platformu üzerinden yedekleme seçenekleri sunmalıdır.</i>	
4.8.	The Software must provide internal command-line (PowerShell) Support.	<i>Yazılım dahili komut satırı (PowerShell) Desteği sunmalıdır.</i>	
4.9.	The software must provide a file management interface that will allow file transfer between the main server and other servers and computers.	<i>Yazılım ana sunucu ve diğer sunucu ve bilgisayarlar arasında dosya transferini sağlayacak bir dosya yönetim arayüzü sunmalıdır.</i>	
4.10.	The software must provide the ability to move virtual machines over the main server and disk areas. It should be able to do this using Vmware vMotion, Storage vMotion, and/or	<i>Yazılım sanal makinaları ana sunucu ve disk alanları üzerinde taşıma özelliği sunmalıdır. Bu işlemi Vmware vMotion, Storage vMotion ve/veya kendi taşıma teknolojisini kullanarak</i>	

	its own transport technology.	<i>yapabilmelidir.</i>	
4.11.	The Software must offer internal compression and singularization that can be customized or disabled by the user without the need for any agent installation.	<i>Yazılım herhangi bir ajan kurulumu gerektirmeden kullanıcı tarafından özelleştirilebilen veya devre dışı bırakılabilen dahili sıkıştırma ve tekilleştirme sunmalıdır.</i>	
4.12.	The Software should provide the option to receive fast incremental backups for only one Virtual Machine from a backup task with more than one Virtual Machine in it.	<i>Yazılım, içerisinde birden fazla Sanal Makina bulunan bir backup görevi içerisinde sadece bir Sanal Makina için hızlı artımlı yedek alabilme seçeneği sunmalıdır.</i>	
4.13.	The software must offer a single full and subsequent 'continuously incremental' backup, eliminating the need for a periodic full backup.	<i>Yazılım tek bir tam ve sonrasında 'sürekli artımlı' yedekleme sunarak periyodik full yedek alma ihtiyacını ortadan kaldıracak sentetik tam yedekleme sunmalıdır.</i>	
4.14.	The Software must be able to automatically copy all backups taken to a disk space or backups of selected Virtual Servers from within for the purpose of copying the backup to a second disk space or for long-term archiving purposes.	<i>Yazılım bir disk alanına alınmış yedeklerin tamamını veya içerisinde seçilen Sanal Sunucuların yedeklerini ikinci bir disk alanına yedeğin kopyalanması veya uzun dönem arşivlenmesi amacı ile otomatik olarak kopyalayabilmelidir.</i>	
4.15.	The Software must be able to access backups taken to a disk space, files from Windows or Linux servers to tape units, tape libraries, and Virtual Tape Libraries.	<i>Yazılım bir disk alanına alınmış yedekleri, Windows veya Linux sunucular içerisinde dosyaları teyp ünitelerine, teyp kütüphanelerine ve Sanal Teyp Kütüphanelerine arşivleyebilmelidir.</i>	
4.16.	The Software must be able to identify the Cloud disk service offered by a manufacturer-approved service provider as a backup store where backups will be stored and use this space to store	<i>Yazılım üretici onaylı bir servis sağlayıcı tarafından sunulan Bulut disk hizmetini, yedeklerin saklanacağı bir yedek deposu olarak tanımlayabilmeli ve bu alanı yedekleri veya yedeklerin kopyalarını saklama amaçlı</i>	

	backups or copies of backups.	<i>kullanabilmelidir.</i>	
4.17.	The software must be able to encrypt stored backups and network traffic end-to-end (when transferring, transferring, and storing) AES256bit.	<i>Yazılım saklanan yedekleri ve ağ trafiğini uçtan uca (kaynakta, aktarırken ve depolarken) AES256bit şifreleyebilmelidir.</i>	
4.18.	The Software should be able to fully back up Virtual Machine, vApp, and metadata directly through the Vmware vCloud Director structure and restore the same components to their original location or on a different vCloud Director structure.	<i>Yazılım Vmware vCloud Director yapısı üzerinden Sanal Makina, vApp ve metadata'ları doğrudan tam yedekleyebilmeli ve aynı bileşenleri orjinal yerlerine ya da farklı bir vCloud Director yapısı üzerine geri yükleyebilmelidir.</i>	
4.19.	The software must be able to perform application-consistent image-based replication of virtual machines running on the Microsoft Hyper-V and VMware vSphere virtualization platform.	<i>Yazılım Microsoft Hyper-V ve Vmware vSphere sanallaştırma platformunda çalışan sanal makinelerin uygulama tutarlı imaj tabanlı replikasyonunu yapabilmelidir.</i>	
4.20.	The Software must be able to operate the Virtual Server replicated on a master server from the desired return point with predefined Virtual Network settings.	<i>Yazılım bir ana sunucu üzerine replike edilmiş Sanal Sunucuyu istenilen geri dönüş noktasından, önceden tanımlanmış Sanal Ağ ayarları ile çalışır duruma getirebilmelidir.</i>	
4.21.	The Software must be able to operate the Virtual Machine with the Microsoft Windows operating system replicated on a master server from the desired return point with predefined IP settings.	<i>Yazılım bir ana sunucu üzerine replike edilmiş Microsoft Windows işletim sistemine sahip Sanal Makinayı istenilen geri dönüş noktasından, önceden tanımlanmış IP ayarları ile çalışır duruma getirebilmelidir.</i>	
4.22.	The software should be able to replicate from the received backups and create the replication fallback points from the	<i>Yazılım alınan yedeklerden replikasyon yapabilmeli, replikasyon geri dönüş noktalarını yedek dosyalarından</i>	

	backup files.	<i>oluşturabilmelidir.</i>	
4.23.	The software must provide Planned Transport to organize data center migration without data loss. Virtual Servers within the scope of the plan should be automatically closed in the specified order and the changes should be transferred and made operational in the new location.	<i>Yazılım veri kaybı olmadan veri merkezi taşımaları organize edecek Planlı Taşıma özelliği sunmalıdır. Plan kapsamındaki Sanal Sunucular belirtilen sıraya göre otomatik olarak kapatılmalı, değişiklikler aktararak yeni lokasyonda çalışır hale getirilmelidir.</i>	
4.24.	The software must be able to make a virtual machine operational without the need for additional copying or intervention directly from the full or incremental backup file on the disk.	<i>Yazılım bir sanal makineyi doğrudan diskte bulunan tam veya artımlı yedek dosyasından ilave bir kopyalama veya müdahaleye gerek kalmadan çalışır duruma getirebilmelidir.</i>	
4.25.	The software must be able to restore a virtual machine from its full or incremental backup file to its original location or on another master server.	<i>Yazılım bir sanal makineyi tam veya artımlı yedek dosyasından orjinal yerine veya başka bir ana sunucu üzerine geri yükleyebilmelidir.</i>	
4.26.	When restoring a virtual machine from backup, the software should offer quick recovery by simply transferring the changing blocks.	<i>Yazılım bir sanal makineyi yedekten geri yüklerken sadece değişen blokları aktararak hızlı kurtarma özelliği sunmalıdır.</i>	
4.27.	The software must be able to restore the files of a virtual machine on the main server.	<i>Yazılım bir sanal makinenin ana sunucu üzerindeki dosyalarını geri yükleyebilmelidir.</i>	
4.28.	The software must be able to independently restore the selected virtual disks of a virtual machine.	<i>Yazılım bir sanal makinenin seçilen sanal diskleri bağımsız olarak geri yükleyebilmelidir.</i>	
4.29.	The Software must be able to restore the Complete Virtual Machine, a file from within the virtual machine, Microsoft Exchange, Active Directory,	<i>Yazılım HP 3PAR StoreServ, HP StoreVirtual, HP StoreVirtual VSA ile NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge ve</i>	

	SharePoint application elements, and Microsoft SQL Databases from within snapshots on the HP 3PAR StoreServ, HP StoreVirtual VSA, and NetApp Data ONTAP-based NetApp FAS, NetApp FlexArray (V-Series), NetAppData ONTAP Edge, and IBM N Series Data Storage units.	<i>IBM N Serisi Veri Depolama ünitelerinin üzerindeki Snapshot'ların içerisinde Komple Sanal Makinayı, Sanal makinanın içinden bir dosyayı, Microsoft Exchange, Active Directory, SharePoint uygulama öğelerini ve Microsoft SQL Veri tabanlarını geri yükleyebilmelidir.</i>	
4.30.	The Software Application must be able to create a second backup on top of NetApp Data ONTAP-based NetApp FAS, NetApp FlexArray (V-Series), NetAppData ONTAP Edge VSA, and IBM N Series Data Storage using consistent NetApp Hardware Snapshots.	<i>Yazılım Uygulama tutarlı NetApp Donanımsal Snapshot'larını kullanarak NetApp Data ONTAP tabanlı NetApp FAS, NetApp FlexArray (V-Serisi), NetAppData ONTAP Edge VSA ve IBM N Serisi Veri Depolama ünitelerinin üzerine ikinci bir yedek oluşturabilmelidir.</i>	
4.31.	The software must be able to export groups, users, and computer accounts from within Microsoft Active Directory backups in LDIFDE format.	<i>Yazılım Microsoft Active Directory yedekleri içerisinde grupları, kullanıcıları ve bilgisayar hesaplarını LDIFDE formatında dışarı aktarabilmelidir.</i>	
4.32.	The Software must provide the ability to quickly search, find, .msg, or export e-mail items, contacts, or notes, including those permanently deleted from Microsoft Exchange 2010 and 2013 server backups, as files or email attachments with the .pst extension.	<i>Yazılım Microsoft Exchange 2010 ve 2013 sunucu yedekleri içerisinde kalıcı olarak silinmiş olanlar dahil e-posta, takvim öğesi, kişi veya notları hızlıca arama, bulma, .msg veya .pst uzantılı dosya veya eposta eklentisi olarak dışarı aktarma olanağı sunulmalıdır.</i>	
4.33.	The Software Microsoft SharePoint 2010 and 2013 server backups must provide the ability to quickly search, find, file, or export items and content as a file or email attachments.	<i>Yazılım Microsoft SharePoint 2010 ve 2013 sunucu yedekleri öğeleri ve içerikleri hızlıca arama, bulma, dosya veya eposta eklentisi olarak dışarı aktarma olanağı sunulmalıdır.</i>	

4.34.	The software must be able to restore databases from microsoft sql server backups to the local database server	Yazılım Microsoft SQL Sunucu yedekleri içerisinde yerel veritabanı sunucusuna geri yükleyebilmelidir	
4.35.	The software should be able to integrate into the vSphere Web Client, instant-speed backups should be started here, information such as the status of the backups, unprotected virtual machines should be accessible directly from within the web client.	Yazılım vSphere Web Client'a entegre olabilmeli, anlık hızlı yedeklemeler buradan başlatılabilmeli, yedeklerin durumları, korunmayan sanal makineler gibi bilgilere doğrudan web client içerisinde erişilebilmelidir.	
4.36.	The Software should be able to import its configuration backup into defined disk space without any user intervention and be restored to include all settings and definitions.	Yazılım kendi konfigürasyon yedeğini herhangi bir kullanıcı müdahalesi gerekmeden tanımlı disk alanına alabilmeli ve tüm ayarları ve tanımlamaları içerecek şekilde geri yüklenebilmelidir.	
4.37.	The software must be licensed for the main server environment consisting of 4 physical processors in the environment.	Yazılım ortamdaki 4 fiziksel işlemciden oluşan ana sunucu ortamı için lisanslanmalıdır. işlemci üzerindeki çekirdek (core) sayısı lisans sayısını etkilememelidir.	
Item to be supplied description		Tedarik edilecek ürün tanımı	Offered technical specifications by the Bidder shall be inserted in English Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir
5. Server Software		Sunucu Yazılımı	Brand/Model // Marka/Model:
5.1.	At least 80 core Windows Server 2019 Standard licenses or equivalent must be issued with the proposed servers.	Teklif edilen sunucularla birlikte en az 80 core Windows Server 2019 Standart lisansı ya da eşdeğeri verilmelidir.	
5.2.	At least 20 Windows Server 2019 Cal licenses or equivalent must be issued	Teklif edilen sunucularla birlikte en az 20 adet Windows Server 2019 Cal	

	with the proposed servers.	<i>lisansı ya da eşdeğeri verilmelidir.</i>	
5.3.	At least 2 SQL Server 2019 <i>Standard Edition</i> licenses or equivalent must be issued with the proposed servers	<i>Teklif edilen sunucularla birlikte en az 2 adet SQL Server 2019 Standard Edition lisansı ya da eşdeğeri verilmelidir</i>	
5.4.	At least 20 SQL Server 2019 Cal licenses or equivalent must be issued with the proposed servers.	<i>Teklif edilen sunucularla birlikte en az 20 adet SQL Server 2019 Cal lisansı ya da eşdeğeri verilmelidir.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
6. Backup Unit		<i>Yedekleme Ünitesi</i>	Brand/Model // <i>Marka/Model:</i>
6.1.	The product to be offered will be the storage unit NAS device that can be connected to the network.	<i>Teklif edilecek ürün ağa bağlanabilen depolama ünitesi NAS cihazı olacaktır.</i>	
6.2.	The data backup unit to be offered will be rack-type attachable to rack cabinets.	<i>Teklif edilecek veri yedekleme ünitesi raf tipinde rack kabinlerine takılabilir yapıda olacaktır.</i>	
6.3.	The proposed product must have at least 8 3.5" disc slots. With the addition of disc drawers, 20 3.5" disc slots should be able to be accessed.	<i>Teklif edilen üründe en az 8 adet 3,5" disk yuvası bulunmalıdır. Disk çekmecesini ilavesi ile 20 adet 3,5" disk yuvasına çıkabilmelidir.</i>	
6.4.	The proposed product must support 108TB disk capacity.	<i>Teklif edilen ürün 108TB disk kapasitesini desteklemelidir.</i>	
6.5.	With the proposed product, specially manufactured discs will be supplied for AT least 8 NAB capacity 7200 rpm return speed SATA or NL-SAS type NAS devices.	<i>Teklif edilen ürünle birlikte en az 8 adet en az 8 TB kapasiteli 7200 rpm dönüş hızında SATA veya NL-SAS tipinde NAS cihazları için özel üretilmiş diskler verilecektir.</i>	
6.6.	The system memory of the proposed product must be	<i>Teklif edilen ürünün sistem belleği en az 2 GB DDR3</i>	

	at least 2 GB of DDR3. With the addition of the memory module, it should be able to increase to 16 GB capacity.	<i>olmalıdır. Bellek modülü ilavesi ile 16 GB kapasiteye çıkabilmelidir.</i>	
6.7.	The proposed processor architecture must be at least 64 bits, at least four cores must be at least 2.4 GHz.	<i>Teklif edilen işlemci mimarisi en az 64 bit, en az dört çekirdek en az 2.4 GHz olmalıdır.</i>	
6.8.	The proposed product must support 2.5" and 3.5" SATA and SSD discs.	<i>Teklif edilen ürün 2,5" ve 3,5" SATA ve SSD diskleri desteklemelidir.</i>	
6.9.	The proposed product must have at least 2 USB 3.0, at least 1 eSATA, and at least 4 Gigabit Ethernet ports supporting Link Aggregation and Failover.	<i>Teklif edilen ürün üzerinde en az 2 adet USB 3.0, en az 1 adet eSATA ve en az 4 adet Link Aggregation ve Failover destekleyen 1 Gigabit Ethernet portu bulunmalıdır.</i>	
6.10.	The proposed product must have at least 1 PCIe Expansion slot.	<i>Teklif edilen ürünün en az 1 adet PCIe Genişletme slotu bulunmalıdır.</i>	
6.11.	The product to be offered will have a power adapter with a power of at least 250W.	<i>Teklif edilecek olan ürünün en 250W gücünde güç adaptörü bulunacaktır.</i>	
6.12.	The device must be able to operate at temperatures from at least 5 °C to a maximum of 35 °C.	<i>Cihaz en az 5 °C ile en fazla 35 °C arasındaki sıcaklıklarda çalışabilmelidir.</i>	
6.13.	The warranty period of the device must be at least 3 years.	<i>Cihazın garanti süresi en az 3 yıl olmalıdır.</i>	
6.14.	The proposed product must support at least 512 folder shares.	<i>Teklif edilen ürün En az 512 adede kadar klasör paylaşımını desteklemelidir.</i>	
6.15.	The number of products iSCSI targets on offer must be at least 128 pieces.	<i>Teklif edilen ürün iSCSI hedef sayısı en az 128 adet olmalıdır.</i>	
6.16.	The number of iSCSI luns on offer must be at least 256 pieces.	<i>Teklif edilen ürün iSCSI lun sayısı en az 256 adet olmalıdır.</i>	
6.17.	The proposed product must support CIFS, AFP, NFS, FTP, WebDAV file protocols.	<i>Teklif edilen ürün CIFS,AFP,NFS,FTP,WebDAV dosya protokollerini desteklemelidir.</i>	
6.18.	The proposed product must support RAID 0, RAID	<i>Teklif edilen ürün RAID 0, RAID 1, RAID 5, RAID 6 ve RAID 10</i>	

	1, RAID 5, RAID 6, and RAID 10 builds.	<i>yapılarını desteklemelidir.</i>	
6.19.	The proposed product must support at least 2048 local user accounts.	<i>Teklif edilen ürün en az 2048 adet yerel kullanıcı hesabını desteklemelidir.</i>	
6.20.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	<i>Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
7. Network Switch Type 1		<i>Ağ Anahtarı Tip 1</i>	Brand/Model // <i>Marka/Model:</i>
7.1.	At least 4 1/10 GbE SFP/SFP+ slots must be supported in the maximum configuration on the proposed switch.	<i>Teklif edilen anahtar üzerinde maksimum konfigürasyonda en az 4 adet 1/10 GbE SFP/SFP+ yuva desteklenebilmelidir.</i>	
7.2.	At least 4 10G SR SFP+ Modules of the same brand as the manufacturer should be given with the proposed switch.	<i>Teklif edilen anahtar ile üretici ile aynı marka en az 4 adet 10G SR SFP+ Modül verilmelidir.</i>	
7.3.	The "Switching" capacity of the proposed switch must be at least 180 Gbps.	<i>Teklif edilen anahtarın "Switching" kapasitesi en az 180 Gbps olmalıdır.</i>	
7.4.	The "Forwarding" capacity of the proposed switch must be at least 130 million packets per second (Mpps).	<i>Teklif edilen anahtarın "Forwarding" kapasitesi en az 130 million packet per second (Mpps) olmalıdır.</i>	
7.5.	The proposed switch must have at least 48 Copper ports supporting the PoE+ standard at 10/100/1000.	<i>Teklif edilen anahtar üzerinde en az 48 adet 10/100/1000 hızında PoE+ standartını destekleyen Bakır port bulunmalıdır.</i>	
7.6.	The POE power budget of the proposed switch must be at least 370W.	<i>Teklif edilen anahtarın POE güç bütçesi en az 370W olmalıdır.</i>	
7.7.	The proposed switch must have 1 10/100 Mbps RJ-45	<i>Teklif edilen anahtar üzerinde 1 adet 10/100 Mbps RJ-45</i>	

	Ethernet Out of Band management port.	<i>Ethernet Out of Band management portu bulunmalıdır.</i>	
7.8.	The proposed switch must be in the stackable architecture. At least 8 devices must be supported in a stack.	<i>Teklif edilen anahtar yığılanabilir mimaride olmalıdır. Bir yığın içerisinde en az 8 adet cihaz desteklenmelidir.</i>	
7.9.	The stacking bandwidth of the proposed switch must be at least 40 Gbps.	<i>Teklif edilen anahtarın yığınlama bant genişliği en az 40 Gbps olmalıdır.</i>	
7.10.	The proposed switch must be supplied with stacking modules if the cable required for stacking is required.	<i>Teklif edilen anahtar yığınlama için gerekli olan kablo gerekli ise yığınlama modülleri ile verilmelidir.</i>	
7.11.	The unit must be insertable and removable while the stack is running. For this purpose, at least one of the "Online Insertion/Removal" or "Hot Insertion/Removal" features should be supported.	<i>Yığın çalışır durumdayken ünite eklenebilir ve çıkarılabilir özellikte olmalıdır. Bu amaçla "Online Insertion/Removal" veya "Hot Insertion/Removal" özelliklerinden en az birisi desteklenmelidir.</i>	
7.12.	There must be at least 16,000 (sixteen thousand) MAC address support in the address table.	<i>Adres tablosunda en az 16.000 (onaltıbin) adet MAC adresi desteği olmalıdır.</i>	
7.13.	"MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" and " Per Vlan Rapid Spanning Tree + (PVST+)" must be supported on the proposed switch.	<i>Teklif edilen anahtar üzerinde "MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" ve " Per Vlan Rapid Spanning Tree + (PVST+)" desteklenmelidir.</i>	
7.14.	120 ports (Etherchannel/Link Aggregation Group/Trunk Group/Multi Trunk Link) must be created using the IEEE 802.3ad Link Aggregation protocol feature. At least 8 ports must be members of a "Link Aggregation Group".	<i>IEEE 802.3ad Link Aggregation protokolü özelliğini kullanarak 120 adet bağlantı noktası (Etherchannel/Link Aggregation Group/Trunk Group/Multi Link Trunk) oluşturulabilmelidir. Bir "Link Aggregation Group" `a en az 8 adet port üye olabilmelidir.</i>	
7.15.	At least 4000 (four thousand) VLAN	<i>IEEE 802.1Q standardında en az 4000 (dört bin) adet VLAN</i>	

	configurations must be supported in the IEEE 802.1Q standard.	<i>konfigürasyonu desteklenmelidir.</i>	
7.16.	At least one of the "RFC 3176 sFlow" or "Netflow" protocols must be supported in order to perform traffic analysis.	<i>Trafik analizi yapabilmek için "RFC 3176 sFlow" veya "Netflow" protokollerinden en az biri desteklenmelidir.</i>	
7.17.	Static routing, RIPv1/v2, and RIPv6 must be supported for IPv4 and IPv6 protocols.	<i>IPv4 ve IPv6 protokolleri için statik yönlendirme, RIPv1/v2 ve RIPv6 desteklenmelidir.</i>	
7.18.	OSPF v2/v3 dynamic routing protocols must be supported by obtaining a license or software update on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile OSPF v2/v3 dinamik yönlendirme protokolleri desteklenebilmelidir.</i>	
7.19.	At least 1000 (thousand) directional registrations must be supported.	<i>En az 1000 (bin) adet yön kaydı desteklenmelidir.</i>	
7.20.	The "VRRP-E" or "HSRP" gateway must support at least one of the backup protocols by obtaining a license or software update on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile "VRRP-E" veya "HSRP" ağ geçidi yedekleme protokollerinden en az birini desteklemelidir.</i>	
7.21.	MLD snooping v1, v2 must be enabled so that IPv6 multicast traffic can be routed to the necessary interfaces and unnecessary multicast broadcasting can be blocked.	<i>IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping v1, v2 özelliği bulunmalıdır.</i>	
7.22.	PIM-SM (PIM Sparse Mode) and PIM-SSM (Source Specific Multicast) must be supported from dynamic multicast routing protocols with license or software updates on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile dinamik multicast yönlendirme protokollerinden PIM-SM (PIM Sparse Mode) ve PIM-SSM (Source Specific Multicast) desteklenmelidir.</i>	
7.23.	RADIUS and TACACS protocols and identification features should be supported.	<i>RADIUS ve TACACS protokolleri ile kimlik tanımlama özelliklerini desteklenmelidir.</i>	
7.24.	Access checklists must be supported.	<i>Erişim kontrol listeleri desteklenmelidir.</i>	

7.25.	At least one of the "Broadcast, multicast and unknown unicast rate-limiting" or "Storm Control" features must be supported.	<i>"Broadcast, multicast and unknown unicast rate limiting" veya "Storm Control" özelliklerinden en az birisi desteklenmelidir.</i>	
7.26.	DHCP Relay, DHCP Server, and DHCP snooping features must be supported.	<i>DHCP Relay, DHCP Server ve DHCP snooping özelliklerini desteklenmelidir.</i>	
7.27.	The "Dynamic ARP Inspection" feature should be supported to protect against network attacks.	<i>Ağ ataklarına karşı koruma amaçlı "Dynamic ARP Inspection" özelliği desteklenmelidir.</i>	
7.28.	The "BPDU guard" feature must be supported to protect the "Spanning Tree" structure against external attacks.	<i>"Spanning Tree" yapısını dış ataklara karşı korumak için "BPDU guard" özelliği desteklenmelidir.</i>	
7.29.	The "Root Guard" feature must be supported to protect the selected switch from attacks and configuration errors.	<i>"Spanning Tree Root" seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı korumak için "Root Guard" özelliği desteklenmelidir.</i>	
7.30.	At least one of the "Multi-Device Authentication" or "Multidomain Authentication" features must be supported to support more than one 802.1x user per port at the same time.	<i>Port başına aynı anda birden fazla 802.1x kullanıcısının desteklenebilmesi adına "Multi Device Authentication" veya "Multidomain Authentication" özelliklerinden en az birisi desteklenmelidir.</i>	
7.31.	"VLAN Based Mirroring" or "VLAN ACL (VACL)" must be supported.	<i>"VLAN Based Mirroring" veya "VLAN ACL (VACL)" desteklenmelidir.</i>	
7.32.	Support for "Uni-Directional Link Detection (UDLD)" should be available to protect the health of connections between switching devices.	<i>Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı "Uni-Directional Link Detection (UDLD)" desteği bulunmalıdır.</i>	
7.33.	Cisco Discovery Protocol (CDP) or LLDP protocol must be supported to learn about neighboring devices.	<i>Komşu cihazları öğrenebilmek amacıyla Cisco Discovery Protocol (CDP) ya da LLDP protokolünü desteklenmelidir.</i>	

7.34.	Support for the "IEEE 802.1AB LLDP-MED" protocol must be available for automatic settings of edge devices such as IP Phones, such as QoS and VLAN.	IP Telefon gibi uç cihazların QoS ve VLAN gibi ayarlarının otomatik olarak yapılabilmesi için "IEEE 802.1AB LLDP-MED" protokolü desteği bulunmalıdır.	
7.35.	It must have support for marking the values "IEEE 802.1p" and "DSCP".	"IEEE 802.1p" ve "DSCP" değerlerini işaretleme (marking/remarking) desteğine sahip olmalıdır.	
7.36.	At least 8 priority/output queues (Priority/Egress Queue) must be defined.	En az 8 adet öncelik/çıkış kuyruğu (Priority/Egress Queue) tanımlanabilmelidir.	
7.37.	There must be support for applying speed restriction to traffic determined according to the access control list.	Erişim kontrol listesine göre belirlenmiş bir trafiğe hız sınırlama uygulama desteği olmalıdır.	
7.38.	The "SCP Secure Copy" protocol must be supported for secure file transfer purposes.	Güvenli dosya transferi amacıyla "SCP Secure Copy" protokolü desteklenmelidir.	
7.39.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.	
Item to be supplied description		Tedarik edilecek ürün tanımı	Offered technical specifications by the Bidder shall be inserted in English Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir
8. Network Switch Type 2 (NON-POE)		Ağ Anahtarı Tip 2 (POE Olmayan)	Brand/Model // Marka/Model:
8.1.	At least 4 1/10 GbE SFP/SFP+ slots must be supported in the maximum configuration on the proposed switch.	Teklif edilen anahtar üzerinde maksimum konfigürasyonda en az 4 adet 1/10 GbE SFP/SFP+ yuva desteklenebilmelidir.	
8.2.	The "Switching" capacity of the proposed switch must be at least 180 Gbps.	Teklif edilen anahtarın "Switching" kapasitesi en az 180 Gbps olmalıdır.	
8.3.	The "Forwarding" capacity of the proposed switch	Teklif edilen anahtarın "Forwarding" kapasitesi en az	

	must be at least 130 million packets per second (Mpps).	<i>130 million packet per second (Mpps) olmalıdır.</i>	
8.4.	There must be at least 48 10/100/1000 RJ45 Copper ports on the proposed key.	<i>Teklif edilen anahtar üzerinde en az 48 adet 10/100/1000 RJ45 Bakır port bulunmalıdır.</i>	
8.5.	The proposed switch must have 1 10/100 Mbps RJ-45 Ethernet Out of Band management port.	<i>Teklif edilen anahtar üzerinde 1 adet 10/100 Mbps RJ-45 Ethernet Out of Band management portu bulunmalıdır.</i>	
8.6.	The proposed switch must be in the stackable architecture. At least 8 devices must be supported in a stack.	<i>Teklif edilen anahtar yığılanabilir mimaride olmalıdır. Bir yığın içerisinde en az 8 adet cihaz desteklenmelidir.</i>	
8.7.	The stacking bandwidth of the proposed switch must be at least 40 Gbps.	<i>Teklif edilen anahtarın yığınlama bant genişliği en az 40 Gbps olmalıdır.</i>	
8.8.	If the cable required for the proposed switch stacking is required, it must be supplied with stacking modules.	<i>Teklif edilen anahtar yığınlama için gerekli olan kablo gerekli ise yığınlama modülleri ile verilmelidir.</i>	
8.9.	The unit must be insertable and removable while the stack is running. For this purpose, at least one of the "Online Insertion/Removal" or "Hot Insertion/Removal" features should be supported.	<i>Yığın çalışır durumdayken ünite eklenebilir ve çıkarılabilir özellikte olmalıdır. Bu amaçla "Online Insertion/Removal" veya "Hot Insertion/Removal" özelliklerinden en az birisi desteklenmelidir.</i>	
8.10.	There must be at least 16,000 (hexadecimal) MAC address support in the address table.	<i>Adres tablosunda en az 16.000 (onaltıbin) adet MAC adresi destegi olmalıdır.</i>	
8.11.	"MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" and " Per Vlan Rapid Spanning Tree + (PVST+)" must be supported on the proposed switch.	<i>Teklif edilen anahtar üzerinde "MST (Multiple Spanning Tree)", "Per Vlan Rapid Spanning Tree (PRST)" ve " Per Vlan Rapid Spanning Tree + (PVST+)" desteklenmelidir.</i>	
8.12.	120 ports (Etherchannel/Link Aggregation Group/Trunk Group/Multi Trunk Link)	<i>IEEE 802.3ad Link Aggregation protokolü özelliğini kullanarak 120 adet bağlantı noktası (Etherchannel/Link</i>	

	must be created using the IEEE 802.3ad Link Aggregation protocol feature. At least 8 ports must be members of a "Link Aggregation Group".	<i>Aggregation Group/Trunk Group/Multi Link Trunk) oluşturulabilmelidir. Bir "Link Aggregation Group" `a en az 8 adet port üye olabilmelidir.</i>	
8.13.	At least 4000 (four thousand) VLAN configurations must be supported in the IEEE 802.1Q standard.	<i>IEEE 802.1Q standardında en az 4000 (dört bin) adet VLAN konfigürasyonu desteklenmelidir.</i>	
8.14.	At least one of the "RFC 3176 sFlow" or "Netflow" protocols must be supported in order to perform traffic analysis.	<i>Trafik analizi yapabilmek için "RFC 3176 sFlow" veya "Netflow" protokollerinden en az biri desteklenmelidir.</i>	
8.15.	Static routing, RIPv1/v2, and RIPv6 must be supported for IPv4 and IPv6 protocols.	<i>IPv4 ve IPv6 protokolleri için statik yönlendirme, RIPv1/v2 ve RIPv6 desteklenmelidir.</i>	
8.16.	OSPF v2/v3 dynamic routing protocols must be supported by obtaining a license or software update on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile OSPF v2/v3 dinamik yönlendirme protokolleri desteklenebilmelidir.</i>	
8.17.	At least 1000 (thousand) directional registrations must be supported.	<i>En az 1000 (bin) adet yön kaydı desteklenmelidir.</i>	
8.18.	The "VRRP-E" or "HSRP" gateway must support at least one of the backup protocols by obtaining a license or updating software on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile "VRRP-E" veya "HSRP" ağ geçidi yedekleme protokollerinden en az birini desteklemelidir.</i>	
8.19.	PIM-SM (PIM Sparse Mode) and PIM-SSM (Source Specific Multicast) must be supported from dynamic multicast routing protocols with license or software update on request.	<i>İstendiğinde lisans alınarak veya yazılım güncellemesi ile dinamik multicast yönlendirme protokollerinden PIM-SM (PIM Sparse Mode) ve PIM-SSM (Source Specific Multicast) desteklenmelidir.</i>	
8.20.	MLD snooping v1, v2 must be enabled so that IPv6 multicast traffic can be routed to the necessary interfaces and unnecessary multicast broadcasting can	<i>IPv6 multicast trafiğinin gerekli arayüzlere yönlendirilebilmesi ve gereksiz multicast yayının engellenebilmesi için MLD snooping v1, v2 özelliği</i>	

	be blocked.	<i>bulunmalıdır.</i>	
8.21.	RADIUS and TACACS protocols and identification features should be supported.	<i>RADIUS ve TACACS protokolleri ile kimlik tanımlama özelliklerini desteklenmelidir.</i>	
8.22.	Access checklists must be supported.	<i>Erişim kontrol listeleri desteklenmelidir.</i>	
8.23.	At least one of the "Broadcast, multicast and unknown unicast rate limiting" or "Storm Control" features must be supported.	<i>"Broadcast, multicast and unknown unicast rate limiting" veya "Storm Control" özelliklerinden en az birisi desteklenmelidir.</i>	
8.24.	DHCP Relay, DHCP Server, and DHCP snooping features must be supported.	<i>DHCP Relay, DHCP Server ve DHCP snooping özelliklerini desteklenmelidir.</i>	
8.25.	The "Dynamic ARP Inspection" feature should be supported to protect against network attacks.	<i>Ağ ataklarına karşı koruma amaçlı "Dynamic ARP Inspection" özelliği desteklenmelidir.</i>	
8.26.	The "BPDU guard" feature must be supported to protect the "Spanning Tree" structure against external attacks.	<i>"Spanning Tree" yapısını dış ataklara karşı korumak için "BPDU guard" özelliği desteklenmelidir.</i>	
8.27.	The "Root Guard" feature must be supported to protect the selected key from attacks and configuration errors.	<i>"Spanning Tree Root" seçilmiş anahtarı ataklara ve yapılandırma hatalarına karşı korumak için "Root Guard" özelliği desteklenmelidir.</i>	
8.28.	At least one of the "Multi Device Authentication" or "Multidomain Authentication" features must be supported to support more than one 802.1x user per port at the same time.	<i>Port başına aynı anda birden fazla 802.1x kullanıcısının desteklenebilmesi adına "Multi Device Authentication" veya "Multidomain Authentication" özelliklerinden en az birisi desteklenmelidir.</i>	
8.29.	"VLAN Based Mirroring" or "VLAN ACL (VACL)" must be supported.	<i>"VLAN Based Mirroring" veya "VLAN ACL (VACL)" desteklenmelidir.</i>	
8.30.	Support for "Uni-Directional Link Detection (UDLD)" should be available to protect the health of connections	<i>Anahtarlama cihazları arasındaki bağlantıların sağlığının korunması amaçlı "Uni-Directional Link Detection (UDLD)" desteği</i>	

	between switching devices.	<i>bulunmalıdır.</i>	
8.31.	Cisco Discovery Protocol (CDP) must support CDP or LLDP protocol in order to learn about neighboring devices.	<i>Komşu cihazları öğrenebilmek amacıyla Cisco Discovery Protocol (CDP) ya da LLDP protokolünü desteklemelidir.</i>	
8.32.	Support for the "IEEE 802.1AB LLDP-MED" protocol must be available for automatic settings of edge devices such as IP Phones, such as QoS and VLAN.	<i>IP Telefon gibi uç cihazların QoS ve VLAN gibi ayarlarının otomatik olarak yapılabilmesi için "IEEE 802.1AB LLDP-MED" protokolü desteği bulunmalıdır.</i>	
8.33.	Must have support for marking the values "IEEE 802.1p" and "DSCP".	<i>"IEEE 802.1p" ve "DSCP" değerlerini işaretleme (marking/remarking) desteğine sahip olmalıdır.</i>	
8.34.	At least 8 priority/output queues (Priority/Egress Queue) must be defined.	<i>En az 8 adet öncelik/çıkış kuyruğu (Priority/Egress Queue) tanımlanabilmelidir.</i>	
8.35.	There must be support for applying speed restriction to traffic determined according to the access control list.	<i>Erişim kontrol listesine göre belirlenmiş bir trafiğe hız sınırlama uygulama desteği olmalıdır.</i>	
8.36.	The "SCP Secure Copy" protocol must be supported for secure file transfer purposes.	<i>Güvenli dosya transferi amacıyla "SCP Secure Copy" protokolü desteklenmelidir.</i>	
8.37.	The proposed product will be guaranteed by the manufacturer the next day for at least 3 years.	<i>Teklif edilen ürün en az 3 yıl boyunca ertesi gün üretici garantili olacaktır.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
9. Wireless Access Point		<i>Kablosuz Erişim Noktası</i>	Brand/Model // <i>Marka/Model:</i>
9.1.	It should be able to operate simultaneously in 2.4GHz and 5 GHz	<i>2.4GHz ve 5 GHz Frekans bantlarında aynı anda çalışabilmelidir.</i>	

	Frequency bands.		
9.2.	12.2. IEEE must support 802.11b/g/a/n/ac wave 2 standards.	<i>IEEE 802.11b/g/a/n/ac wave 2 standartlarını desteklemelidir.</i>	
9.3.	12.3. 802.11n technology should support 20 MHz, and 40 Mhz signals in both 2.4 GHz and 5 GHz bands. 80 MHz signal should support 5 GHz signal in 802.11ac technology.	<i>802.11n teknolojisinde hem 2.4 GHz hem de 5 GHz bantlarında 20 MHz, ve 40 Mhz sinyalleri desteklemelidir. 802.11ac teknolojisinde 5 GHz bandında 80 MHz sinyali desteklemelidir.</i>	
9.4.	12.4. The following performance values must be supported: a) 802.11ac: 6.5 Mbps – 867 Mbps b) 802.11n: 6.5Mbps – 300 Mbps c) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps d) 802.11b: 11, 5.5, 2, 1 Mbps	<i>Aşağıdaki performans değerleri desteklenmelidir: a) 802.11ac: 6.5 Mbps – 867 Mbps b) 802.11n: 6.5Mbps – 300 Mbps c) 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps d) 802.11b: 11, 5.5, 2, 1 Mbps</i>	
9.5.	Support Transmit BeamForming technology.	<i>Transmit BeamForming teknolojisini desteklemelidir.</i>	
9.6.	It must have intelligent antenna technology that can dynamically shape the broadcast area and provide advanced RF management by changing antenna coverage. 128 different broadcast areas must be dynamically created. In this way, an additional gain of 4 dB should be achieved in the direction of Transmit to antenna power. Thanks to the dynamically shaped broadcast area, signals should not be sent in directions where there is no communication, such broadcasts should be weakened at a rate of 10 dB.	<i>Dinamik olarak yayın alanını şekillendirebilen akıllı bir anten teknolojisine sahip olmalı ve anten kapsama alanlarını değiştirerek ileri düzey RF yönetimi sağlamalıdır. 128 farklı yayın alanı dinamik olarak yaratılabilmelidir. Bu sayede anten gücüne Transmit yönünde 4 dB ilave kazanç sağlanabilmelidir. Dinamik olarak şekillendirilebilen yayın alanı sayesinde haberleşmenin olmadığı yönlerde sinyal gönderilmemeli, bu tür yayınlar 10 dB oranında zayıflatılmalıdır.</i>	
9.7.	Radio Frequency output	<i>Radyo Frekansı çıkış gücü 2.4</i>	

	power should be 23 dBm for 2.4 GHz and 23 dBm for 5 GHz.	<i>GHz için 23 dBm, 5 GHz için 23 dBm olmalıdır.</i>	
9.8.	Reception sensitivity must be up to -101 dBm.	<i>Alış hassasiyeti -101 dBm'e kadar olmalıdır.</i>	
9.9.	Must have at least 2x2 MIMO antenna structure.	<i>En az 2x2 MIMO anten yapısına sahip olmalıdır.</i>	
9.10.	At least 2 Spatial-Streams must be supported.	<i>En az 2 Spatial-Stream desteklenmelidir.</i>	
9.11.	Support 256 users at the same time.	<i>Aynı anda 256 kullanıcı desteklemelidir.</i>	
9.12.	The channel must be able to select automatically.	<i>Kanal seçimini otomatik yapabilmelidir.</i>	
9.13.	Background Scanning should allow you to detect interference (interference) in high-density environments and automatically select the appropriate channel by avoiding them.	<i>Background Scanning yaparak yüksek yoğunluklu ortamlardaki girişimleri (paraziti) tespit edebilme ve bunlardan sakınarak uygun kanalı otomatik olarak seçme özelliği bulunmalıdır.</i>	
9.14.	IP multicast video stream support must be available.	<i>IP multicast video stream desteği bulunmalıdır.</i>	
9.15.	IPv6 support must be available.	<i>IPv6 desteği bulunmalıdır.</i>	
9.16.	The device should be able to analyze packages automatically and assign them to the relevant queues using advanced service quality, packet classification, and automatic prioritization for latency-sensitive traffic.	<i>Cihaz paketleri otomatik olarak analiz edebilmeli, gecikmeye duyarlı trafik için ileri düzey servis kalitesi, paket sınıflandırma ve otomatik öncelik belirleme özelliklerini kullanarak bunları ilgili kuyruklara atayabilmelidir.</i>	
9.17.	There should be fair airtime fairness support.	<i>Adil yayın zamanı kullanım desteği (Airtime Fairness) olmalıdır.</i>	
9.18.	It should have the ability to automatically detect the highest performance channel and adjust itself to it. It should not interrupt communication with computers when scanning all channels for the purpose of detecting the highest performance channel.	<i>En yüksek performanslı kanalı otomatik olarak tespit edip kendisini o kanala ayarlama özelliği olmalıdır. En yüksek performanslı kanalı tespit amacıyla tüm kanalları tararken bilgisayarlarla olan iletişimi kesmemelidir.</i>	

9.19.	It should have VLAN support.	<i>VLAN desteği olmalıdır.</i>	
9.20.	WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i must support security features.	<i>WEP, WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i güvenlik özelliklerini desteklemelidir.</i>	
9.21.	Support port-based 802.1x security features over RADIUS (both authenticator and supplicant).	<i>Port tabanlı 802.1x güvenlik özelliklerini RADIUS üzerinden desteklemelidir (hem authenticator hem de supplicant olarak).</i>	
9.22.	It should have BandSteering capability and be able to force both 2.4 GHz and 5 GHz supported computers to connect over 5 GHz for load sharing when necessary.	<i>BandSteering özelliği olmalı ve gerekli gördüğünde yük paylaşımı için hem 2.4 GHz hem de 5 GHz destekli bilgisayarları öncelikle 5 GHz üzerinden bağlanmaya zorlayabilmelidir.</i>	
9.23.	16 BSSIDs should be supported where security and service quality policies can be set separately.	<i>Güvenlik ve servis kalitesi politikalarının ayrı ayrı ayarlanabileceği 16 adet BSSID desteklenmelidir.</i>	
9.24.	Support router feature including NAT and DHCP services.	<i>NAT ve DHCP servislerini de içeren router özelliğini desteklemelidir.</i>	
9.25.	HotSpot WLAN must dynamically have a user-by-user speed restriction feature.	<i>HotSpot WLAN için dinamik olarak kullanıcı bazında hız kısıtlama özelliği olmalıdır.</i>	
9.26.	It must be configured independently from the command line (Telnet/SSH), web interface (http/s), via Controller switch, via SNMP v1,2,3 software. Must support TR-069.	<i>Bağımsız olarak komut satırından (Telnet/SSH), Web ara-yüzünden (http/s), Controller switch üzerinden, SNMP v1,2,3 yazılımı üzerinden konfigürasyonu yapılabilirdir. TR-069 desteği olmalıdır.</i>	
9.27.	Be able to make software updates with FTP and TFTP.	<i>FTP ve TFTP ile yazılım güncellemeleri yapabilmelidir.</i>	
9.28.	It must be able to operate independently or in a controller control.	<i>Bağımsız olarak veya bir controller denetiminde çalışabilmelidir.</i>	
9.29.	When working independently, L2TP must be able to tunnel between it and the head office.	<i>Bağımsız olarak çalışırken merkez ofisle arasında L2TP tünel oluşturabilmelidir.</i>	

9.30.	When used with the controller it must support the following features: a) Authentication must be performed through the local database on the controller, via Active Directory, LDAP, or RADIUS server. b) Access control and load sharing between AP devices. c) Captive Portal and Guest user accounts that can authenticate over the web should be supported. d) In order to be able to roam quickly in voip and 802.1x EAP related applications, a tunnel must be established between the controller and the AP.	<i>Controller ile birlikte kullanıldığında aşağıdaki özellikleri desteklemelidir:</i> i. <i>Kimlik doğrulama işlemleri controller üzerindeki yerel veri tabanı üzerinden, Active Directory, LDAP veya RADIUS server üzerinden yapabilmelidir.</i> ii. <i>Erişim kontrolü ve AP cihazları arasında yük paylaşımı olmalıdır.</i> iii. <i>Web üzerinden kimlik doğrulaması yapabilen Captive Portal ve Misafir kullanıcı hesapları desteklenmelidir.</i> iv. <i>VoIP ve 802.1x EAP ile ilgili uygulamalarda hızlı roaming yapabilmek için controller ile AP arasında tünel oluşturulabilmelidir.</i>	
9.31.	Must have the following physical characteristics: a) Be able to feed on 12 VDC or PoE. If the DC adapter is received, it must be able to operate between 110-240 VAC. b) Power consumption should be no more than 13W. c) It should be able to operate between 0°C and +40°C. d) Be able to work in relative humidity environments up to 95%. e) Kensington lock against theft should be possible. f) It must have a locking mechanism that will prevent accidental exit/fall from where it is installed. g) There must be one 10/100/1000BaseT Gigabit	<i>Aşağıdaki fiziki özelliklere sahip olmalıdır:</i> a) <i>12 VDC ile veya PoE üzerinden beslenebilmelidir. DC adaptör alınmışsa 110-240 VAC arasında çalışabilmelidir.</i> b) <i>Güç tüketimi en fazla 13W olmalıdır.</i> c) <i>0°C ile +40°C arasında çalışabilmelidir.</i> d) <i>%95'e kadar bağıl nem ortamlarında çalışabilmelidir.</i> e) <i>Çalınmaya karşı Kensington kilit imkânı</i>	

	Ethernet port on it and it must be able to receive electricity via PoE. This port auto MDX should support auto-sensing. h) PoE power requirement must be within 802.3af standards. i) Energy saving feature.	<i>olmalıdır.</i> <i>f) Monte edildiği yerden kazara çıkmayı/düşmeyi engelleyecek bir kilit mekanizmasına sahip olmalıdır.</i> <i>g) Üzerinde bir adet 10/100/1000BaseT Gigabit Ethernet port olmalıdır ve bu port PoE üzerinden elektrik alabilmelidir. Bu port auto MDX, auto-sensing özelliğini desteklemelidir.</i> <i>h) PoE güç ihtiyacı 802.3af standartları içinde olmalıdır.</i> <i>i) Enerji tasarruf özelliği olmalıdır.</i>	
9.32.	Limited lifelong guarantee should be provided against manufacturing and labor defects.	<i>İmalat ve işçilik hatalarına karşı kısıtlı ömür boyu garanti sağlanmalıdır.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
10. Authentication and Network Access Control Software		<i>Kimlik Doğrulama ve Ağ Erişim Kontrol Yazılımı</i>	Brand/Model // <i>Marka/Model:</i>
10.1.	The authentication and network access control platform can be offered to	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, Vmware altyapısı üzerinde çalışacak</i>	

	run on VMware infrastructure or as hardware.	<i>şekilde veya donanım olarak teklif edilebilir.</i>	
10.2.	The authentication and network access control platform must work in full compatibility with the proposed network switches and wireless access devices.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, teklif edilen ağ anahtarları ve kablosuz erişim cihazları ile tam uyumlu çalışmalıdır.</i>	
10.3.	Authentication and network access control platform should not compromise system security, Vlan assignment, profiling, etc. In order to use its features, it should not request SNMP write right.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, sistem güvenliğini tehlikeye düşürmemeli, Vlan ataması, profilendirme vb. özelliklerin kullanılabilmesi amacıyla SNMP yazma (SNMP write) hakkı istememelidir.</i>	
10.4.	Authentication and network access control platform should work using IEEE 802.1x protocol	<i>Kimlik doğrulama ve ağ erişim kontrol platformu, IEEE 802.1x protokolünü kullanarak çalışmalıdır</i>	
10.5.	The authentication and network access control platform should be able to work centrally. No additional hardware or software should be installed in the zones.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu merkezi olarak çalışabilmelidir. Bölgelere ayrıca donanım veya yazılım kurulması gerekmemelidir.</i>	
10.6.	The authentication and network access control platform should be available for both wired and wireless network and VPN.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu hem kablolu hem kablosuz ağ hem de VPN için kullanılabilmelidir.</i>	
10.7.	Authentication and network access control platform should work with RADIUS protocol.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu RADIUS protokolü ile çalışmalıdır.</i>	
10.8.	Authentication and network access control platform should be managed through a single management screen.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu tek bir yönetim ekranı üzerinden yönetilmelidir.</i>	

10.9.	Authentication and network access control platform for the network , including the last, which users / devices identity, group, device make and model, contact tour (wireless is) physically being connected location , post, applications running on running malicious software, if any, etc. must be able to see / learn information and take action accordingly.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu Ağa dahil olan son kullanıcı/cihazların kimlik, grup, cihaz marka ve modeli, bağlantı turu, (kablosuz ise) bağlandığı fiziksel lokasyon, postur, üzerinde çalışan uygulama, varsa üzerinde çalışan zararlı yazılımlar vs. bilgileri görebilmeli/öğrenebilmeli ve bunlara göre aksiyon alabilmelidir.</i>	
10.10.	Authentication and network access control platform should be able to act as NAC, it should be able to determine the current status of the operating system and antivirus application on the client, USB connection, disk encryption, etc. should be able to control.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu NAC görevi yapabilmeli, istemci üzerindeki işletim sistemi ve anti virüs uygulamasının güncellik durumlarını, USB bağlantısını, disk kriptosunu vs. kontrol edebilmelidir.</i>	
10.11.	The authentication and network access control platform must be licensed for at least 500 endpoints . The duration of the offered licenses must be at least 5 years.	<i>Kimlik doğrulama ve ağ erişim kontrol platformu en az 500 endpoint için lisanslanmalıdır. Teklif edilen lisansların süresi en az 5 yıl olmalıdır.</i>	
10.12.	The system to be proposed should be able to work with all network devices that are IEEE 802.1x compliant and independent of the brand.	<i>Teklif edilecek sistem, IEEE 802.1x uyumlu marka bağımsız tüm ağ cihazları ile çalışabilmelidir.</i>	
10.13.	The system to be proposed should be able to authorize MAC for devices that do not support IEEE 802.1x.	<i>Teklif edilecek sistem, IEEE 802.1x desteği olmayan cihazlar için MAC yetkilendirmesi yapabilmelidir.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder

			shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
11. Firewall		<i>Güvenlik Duvarı</i>	Brand/Model // <i>Marka/Model:</i>
11.1.	The proposed system must have at least the following features as the next generation firewall features. • Firewall • IPSec VPN Termination System • SSL VPN Termination System • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control • URL Category Filtering • Bandwidth management	<i>Teklif edilen sistem, yeni nesil güvenlik duvarı özellikleri olarak asgari aşağıdaki özelliklerde olmalıdır.</i> • <i>Güvenlik Duvarı (Firewall)</i> • <i>IPSec VPN Sonlandırma Sistemi</i> • <i>SSL VPN Sonlandırma Sistemi</i> • <i>Saldırı Tespit ve Engelleme Sistemi (IPS)</i> • <i>Uygulama Tanıma ve Kontrolü (Application Control) Sistemi</i> • <i>Virüs/Zararlı İçerik Kontrolü</i> • <i>URL Kategorisi Filtreleme</i> • <i>Bant genişliği yönetimi</i>	
11.2.	These features should be provided with a single device as a hardware solution of the	<i>Bu özellikleri üreticiye ait donanımsal çözüm olarak tek bir cihaz ile sağlanmalıdır. Fakat IPSec VPN ve SSL VPN</i>	

	manufacturer. However, in case IPSec VPN and SSL VPN features cannot be supported when positioned Transparent; It can be provided with the virtual firewall feature on the same system or with a separate hardware product from the same manufacturer.	<i>özelliklerinin Transparen konumlandırıldığında desteklenememesi durumunda; aynı sistem üzerinde sanal güvenlik duvarı özelliği ile veya aynı üreticiye ait ayrı bir donanımsal ürün ile sağlanabilir.</i>	
11.3.	The device can operate as a single physical firewall, and in any case, it must be configured to run at least 10 virtual firewalls if the organization needs it.	<i>Cihaz tek bir fiziksel güvenlik duvarı olarak çalışabileceği gibi, her halukarda kurumun ihtiyaç duyması durumunda en az 10 adet sanal güvenlik duvarı çalıştıracak şekilde konfigüre edilebilmelidir.</i>	
11.4.	The proposed Network Firewall must support Active-Active and Active-Passive operation for High-Availability. It should be able to share load while Active-Active. In case of failure of one of the devices, the other device should be able to continue operating by undertaking all functions.	<i>Teklif edilen Ağ Güvenlik Duvarı, High-Availability için Aktif-Aktif ve Aktif-Pasif olarak çalışmayı desteklemelidir. Aktif-Aktif çalışırken yük paylaşımı yapabilmelidir. Cihazlardan birinin arızalanması durumunda, diğer cihaz tüm fonksiyonları üstlenerek çalışmaya devam edebilmelidir.</i>	
11.5.	The system must have SPI (Stateful Packet Inspection) Firewall feature.	<i>Sistemin SPI (Stateful Packet Inspection) Firewall özelliği olmalıdır.</i>	
11.6.	The system will detect and block spoofed packets.	<i>Sistem, spoof edilmiş paketleri tespit edip bloklayacaktır.</i>	
11.7.	Each of the network interfaces in the system; It must be able to be defined as LAN, WAN, DMZ, or user-nameable segments. The system should support IEEE 802.1Q VLAN and defined VLANs should be used as an interface.	<i>Sistemde bulunan ağ arayüzlerinin her biri; LAN, WAN, DMZ, veya kullanıcı tarafından isimlendirilebilen segmentler olarak tanımlanabilmelidir. Sistem IEEE 802.1Q VLAN desteklemeli ve tanımlanan VLAN'lar arayüz (interface) olarak kullanılabilmelidir</i>	

11.8.	When offered with System Virtual Firewall feature; Physical and virtual interfaces on the system should be able to be shared between Virtual Firewalls. Virtual Firewalls should be managed independently from each other in terms of rules and routing.	<i>Sistem Sanal Güvenlik Duvarı özelliği ile teklif edildiği durumda; sistem üzerindeki fiziksel ve sanal ara yüzler Sanal Güvenlik Duvarları arasında paylaştırılabilir. Sanal Güvenlik Duvarları kural ve yönlendirme açısından birbirinden bağımsız olarak yönetilebilir.</i>	
11.9.	System; It must be able to work on Layer3 (routing mode) and Layer2 (transparent mode) layers. While the desired virtual firewall systems on the system can work in Layer3, the desired virtual firewalls must be able to work transparently on Layer2 at the same time.	<i>Sistem; Layer3 (routing mod) ve Layer2 (saydam mod) katmanlarında çalışabilir. Sistem üzerinde sanal güvenlik duvarı sistemlerinden istenilenler Layer3 te çalışabilirken aynı anda istenilen sanal güvenlik duvarları Layer2 de transparant olarak çalışabilir.</i>	
11.10.	It should provide the following features in Transparent mode: • SPI (stateful packet inspection), • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control on Gateway • URL Category Filtering	<i>Saydam (Transparent) modda aşağıdaki özellikleri sağlamalıdır:</i> • SPI (stateful packet inspection), • Saldırı Tespit ve Engelleme Sistemi (IPS) • Uygulama Tanıma ve Kontrolü (Application Control) Sistemi • Ağ Geçidinde Virüs/Zararlı İçerik Kontrolü • URL Kategori Filtreleme	
11.11.	In routing mode, it should provide the following	<i>Routing modda aşağıdaki özellikleri sağlamalıdır;</i>	

	features: • SPI (stateful packet inspection), • IPSec VPN Termination, • SSL VPN Termination, • Intrusion Detection and Prevention System (IPS) • Application Recognition and Control System • Virus / Malicious Content Control • URL Category Filtering • Bandwidth control • Static routing, • RIP must support OSPF and BGP routing protocols. If a license or extra software is required to provide these routing protocols, it must have been provided. • Server load	• SPI (stateful packet inspection), • IPSec VPN Sonlandırma, • SSL VPN Sonlandırma, • Saldırı Tespit ve Engelleme Sistemi (IPS) • Uygulama Tanıma ve Kontrolü (Application Control) Sistemi • Virüs/Zararlı İçerik Kontrolü • URL Kategori Filtreleme • Bant genişliği kontrolü • Statik yönlendirme (static routing), • RIP, OSPF ve BGP yönlendirme protokollerini desteklemelidir. Bu yönlendirme protokollerini sağlamak için lisans veya fazladan yazılım gerekiyorsa sağlanmış olmalıdır. • Sunucu yük dengeleme • WIFI Access Point	
--	--	---	--

	balancing - WIFI Access Point controller - WAN optimization	<i>kontrolcüsü</i> <i>WAN optimizasyon</i>	
11.12.	The Network Security System should support multiple Wide Area Network (WAN) connections, and be able to use more than one Internet connection as redundant.	<i>Ağ Güvenlik Sisteminin, Birden fazla Geniş Alan Ağı (WAN) bağlantısını desteklemeli, birden fazla Internet bağlantısını yedekli olarak kullanabilmelidir.</i>	
11.13.	Network Security System must support Policy Based Routing.	<i>Ağ Güvenlik Sistemi, Kural Tabanlı Yönlendirmeyi (Policy Based Routing) desteklemelidir.</i>	
11.14.	The system must have DHCP Server and DHCP Relay feature.	<i>Sistemin DHCP Server ve DHCP Relay özelliği bulunmalıdır.</i>	
11.15.	Firewall policies should be able to be written on the network interface and / or zone basis on the system.	<i>Güvenlik duvarı politikaları sistem üzerindeki ağ arayüzü ve/veya zone bazlı yazılabilmelidir.</i>	
11.16.	Firewall policies should be written on the basis of user and user groups. Must have AD integration for user information.	<i>Güvenlik duvarı politikaları, kullanıcı ve kullanıcı grupları bazında yazılabilmelidir. Kullanıcı bilgisi için AD entegrasyonu olmalıdır.</i>	
11.17.	The system should be able to do rule-based traffic shaping and traffic prioritization for Bandwidth Control. The system must support QoS and Differentiated Services. Traffic formatting should also be defined in rules written on the basis of source,	<i>Sistem Bant Genişliği Kontrolü amacıyla kural tabanlı trafik biçimlendirme, ve trafik önceliklendirme yapabilmelidir. Sistem QoS ve Differentiated Services desteklemelidir.</i> <i>Kaynak, hedef, ve protokol (SMTP, FTP, DNS, H323 gibi) bazında yazılan kurallarda trafik biçimlendirme tanımı</i>	

	destination, and protocol (such as SMTP, FTP, DNS, H323). • The maximum and / or guaranteed bandwidth value should be defined by priority value (such as low, medium, high). • Bandwidth control on per-IP basis should be possible when required. In this way, it should be ensured that the bandwidth defined for each resource allowed on the same rule is guaranteed. • Contrary to Article above, it should be ensured that the bandwidth defined for each resource allowed within the same rule can be used in common. • It should be able to control bandwidth	<i>da yapılabilmelidir.</i> • <i>Maksimum ve/veya garanti edilecek bant genişliği değeri öncelik değeri (düşük, orta, yüksek gibi) ile tanımlanabilmelidir.</i> • <i>İstenildiğinde per-IP bazında bant genişliği kontrolü yapılabilmelidir. Bu sayede aynı kural üzerinden izin verilen her kaynak için tanımlanan bant genişliğinin garanti edilmesi sağlanmalıdır.</i> • <i>Üstteki maddenin aksine tüm aynı kural dahilinde izin verilen her kaynak için tanımlanan bant genişliğinin ortak bir şekilde kullanılabilmesi sağlanabilmelidir.</i> • <i>Uygulama bazında bant genişliği kontrolü yapabilmelidir.</i> • <i>Aynı trafik ile ilgili Inbound ve outbound</i>	
--	---	--	--

	on the basis of application. Bandwidth control should be possible in inbound and outbound direction for the same traffic. Thus, while bandwidth can be specified in the outbound line for a permitted connection, a different bandwidth should be applied for the traffic corresponding to this connection.	<i>doğrultuda band genişliği kontrolü yapılabilmelidir. Bu sayede izin verilen bir bağlantı için gidiş doğrultusunda bant genişliği belirtilebilirken, bu bağlantıya karşılık gelen trafik için farklı bir bant genişliği uygulanabilmelidir.</i>	
11.18.	Security System; It must be able to authenticate and authorize over the user database defined on it, RADIUS and LDAP.	<i>Güvenlik Sistemi; kendi üzerinde tanımlanan kullanıcı veritabanı, RADIUS ve LDAP üzerinden kimlik doğrulama ve yetkilendirme yapabilmelidir.</i>	
11.19.	The system must have application control feature. System; It should be able to recognize, control and block traffic of at least 3,000 (three thousand) applications, such as messaging (such as MSN, ICQ, Yahoo, AOL), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella, etc.) and Web Applications, regardless of the port used.	<i>Sistemin uygulama kontrol özelliği bulunmalıdır. Sistem; Mesajlaşma (MSN, ICQ, Yahoo, AOL gibi), P2P (Kazaa, Skype, bitTorrent, eDonkey, Gnutella vb) ve Web Uygulamaları gibi tanımlı en az 3.000 (üçbin) adet uygulamaya ait trafiği kullanılan porttan bağımsız olarak tanıyabilmeli, kontrol edebilmeli ve engelleyebilmelidir. Uygulama kontrolü kapsamında tanınan</i>	

	Applications recognized within the scope of application control should be updated with an update service over the internet.	<i>uygulamalar internet üzerinden güncelleme servisi ile güncellenmelidir.</i>	
11.20.	It should be possible to control whether the policy-based firewall logs start / stop in sessions .	<i>Politika bazlı firewall'un oturumlarda start/stop loglayıp / loglamaması denetlenebilmelidir.</i>	
11.21.	Firewall, NAT, and all layer7 security functions provided should be able to be enabled in granular form on a rule-based basis "only for traffic that meets the specified criteria."	<i>Firewall, NAT ve sunulan tüm layer7 güvenlik fonksiyonları granüler şekilde "sadece belirlenen kriterlere uyan trafik için" kural bazlı devreye alınabilmelidir.</i>	
11.22.	Daily operation operations should be able to be performed to a large extent (without the need to operate on the CLI) via WebGUI. On the other hand, the entire configuration should be able to be intervened in bulk via CLI.	<i>WebGUI üzerinden günlük operasyon işlemleri büyük oranda (CLI üzerinde işlem yapmaya gerek olmadan) gerçekleştirilebilmelidir. CLI üzerinden ise tüm konfigürasyona bulk şekilde müdahale edilebilmelidir.</i>	
11.23.	The application control policy should be set in each firewall rule written on the basis of source (IP and / or user), target, service.	<i>Kaynak (IP ve/veya kullanıcı), hedef, servis bazında yazılan her güvenlik duvarı kuralında uygulama kontrol politikası set edilebilmelidir.</i>	
11.24.	The system should support IPSec VPN as VPN Gateway. DES must support MD5 and SHA-1 with 3DES, AES Encryption. There should be support for IKE and PKI. IPSEC VPN functions should be able to perform at hardware level performance on special ASIC-architecture hardware without straining the main resources of the system.	<i>Sistem VPN Gateway olarak IPSec VPN desteklemelidir. DES, 3DES, AES Kriptolama ile MD5 ve SHA-1 desteklemelidir. IKE ve PKI desteği olmalıdır. IPSEC VPN işlevleri ASIC mimarili özel hardware üzerinde sistem ana kaynaklarını yormadan donanımsal seviyede performanslı gerçekleştirilebilmelidir.</i>	

11.25.	The IPS system should be able to detect and stop Traffic and Protocol anomalies , as well as recognize and stop signature-based attacks. IPS signatures should be able to be updated automatically with the update service over the internet. The update process should also be able to be done manually.	<i>IPS sistemi Trafik ve Protokol anomalilerini tespit edip durdurabildiği gibi, imza tabanlı saldırıları da tanıyıp durdurabilmelidir. IPS imzaları otomatik olarak internet üzerinden güncelleme servisi ile güncellenebilmelidir. Güncelleme işlemi manuel olarak ta yapılabilirdir.</i>	
11.26.	It should allow system administrators to create and block weakness signatures specific to the organization / need .	<i>Sistem yöneticilerinin kuruma/ihtiyaca özel zaafiyet imzaları yaratıp bloklama yapabilmelerine imkan sağlamalıdır.</i>	
11.27.	IPS policy should be set in every firewall rule written on the basis of source (IP and / or user), target, service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında IPS politikası set edilebilmelidir.</i>	
11.28.	The proposed Network security system should be able to detect and block Botnet activity.	<i>Teklif edilen Ağ güvenlik sistemi Botnet aktivitesini tespit edip engelleyebilmelidir.</i>	
11.29.	By analyzing the behavior of user traffics, it should allow easy detection of user machines displaying abnormal behavior on the graphical interface. All behaviors between layer3-layer7, such as traffic blocked through the firewall, attempts to access inappropriate web categories, running risky applications, communication with botnet sites, should be determined by weighing determinable scoring. In this way, it is aimed to detect a zero-day activity	<i>Kullanıcı trafiklerinin davranış analizini yaparak, anormal davranış gösteren kullanıcı makinalarının grafiksel arayüzde kolayca tesbitine olanak sağlamalıdır. Firewall üzerinden bloklanan trafikler, uygunsuz web kategorilerine erişim denemeleri, riskli uygulamaların çalışıyor olması, botnet siteleri ile haberleşme gibi layer3-layer7 arası tüm davranışlar ağırlığı belirlenebilir puanlama ile belirlenebilmelidir. Bu sayede henüz imzası yayınlanmamış bir sıfır-gün aktivitesinin tesbit edilmesi amaçlanmaktadır</i>	

	whose signature has not yet been published.		
11.30.	The Network Security System must have SSL VPN Gateway feature in order to provide secure access of Mobile Users to Institution resources. SSL VPN client must support at least Windows, Mac OS, Linux operating systems and IOS, Android based mobile devices.	<i>Ağ Güvenliği Sistemi üzerinde, Mobil Kullanıcıların Kurum kaynaklarına güvenli olarak erişimini sağlayabilmek için, SSL VPN Gateway özelliği bulunmalıdır. SSL VPN istemcisi en az Windows, Mac OS, Linux işletim sistemlerini ve IOS, Android tabanlı mobil cihazları desteklemelidir.</i>	
11.31.	TCP and UDP-based traffic must be tunneled through SSL VPN Gateway.	<i>SSL VPN Gateway içerisinde TCP ve UDP tabanlı trafikler tünellenebilmelidir.</i>	
11.32.	SSL VPN feature will be offered with unlimited user license.	<i>SSL VPN özelliği sınırsız kullanıcı lisansı ile teklif edilecektir.</i>	
11.33.	Users accessing via SSL VPN should be able to authenticate and authorize over the user database defined on the System, RADIUS, LDAP, and define internal and external resources that can be accessed with this authorization.	<i>SSL VPN üzerinden erişen kullanıcılar, Sistem üzerinde tanımlı kullanıcı veritabanı, RADIUS, LDAP üzerinden kimlikleri doğrulanabilmeli, yetkilendirilebilmeli ve bu yetkilendirme ile erişilebilecek kurum içi ve dışı kaynaklar tanımlanabilmelidir.</i>	
11.34.	For users or systems accessing with SSL VPN and IPSEC VPN; SPI (stateful packet inspection), Intrusion Detection and Prevention System (IPS), Application Recognition and Control (Application Control) System, Virus / Malicious Content Control and URL Category Filtering, QoS and Bandwidth management features must be applicable.	<i>SSL VPN ve IPSEC VPN ile erişim sağlayan kullanıcı veya sistemleri için; SPI (stateful packet inspection), Saldırı Tespit ve Engelleme Sistemi (IPS), Uygulama Tanıma ve Kontrolü (Application Control) Sistemi, Virüs/Zararlı İçerik Kontrolü ve URL Kategori Filtreleme, QoS ve Bant Genişliği yönetimi özellikleri uygulanabilir olmalıdır.</i>	
11.35.	Malware detection and blocking feature must be available on the Network Firewall System. System; It	<i>Ağ Güvenlik Duvarı Sistemi üzerinde zararlı yazılım (Malware) tespit ve engelleme özelliği bulunmalıdır. Sistem;</i>	

	should be able to prevent malicious software by scanning HTTP, SMTP, FTP, and POP3, IM (ICQ, MSN, Yahoo Messenger), MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB traffic. The system scans within the aforementioned protocols; It should be able to detect and stop threats such as Worm, Trojan, Keylogger, Spy, Dialer. Virus Control should be able to be performed between all network segments on the Network Firewall System. The AntiVirus system should be able to automatically update virus signatures over the Internet.	<i>HTTP, SMTP, FTP ve POP3, IM (ICQ, MSN, Yahoo Messenger) , MAPI, HTTPS, SMTPS, POP3S, IMAPS, FTPS, SMB trafiğini tarayarak zararlı yazılımları engelleyebilmelidir. Sistem, anılan protokoller içinde tarama yaparak; Worm, Trojan, Keylogger, Spy, Dialer türünden tehditleri tanıyıp durdurabilmelidir. Virüs Kontrolü, Ağ Güvenlik Duvarı Sistemi üzerinde bulunan bütün network segment'leri arasında yapılabilirdir. AntiVirus sistemi Internet üzerinden virüs imzalarını otomatik olarak güncelleyebilmelidir</i>	
11.36.	AV control policy should be set in every firewall rule written on the basis of source (IP and / or user), target, service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında AV kontrol politikası set edilebilmelidir.</i>	
11.37.	There should be URL Filtering feature on the Network Security System. In this way, Category - based URL Filtering should be able to. Different categories of URL filtering should be able to be applied to different users and user groups.	<i>Ağ Güvenliği Sistemi üzerinde URL Filtreleme özelliği bulunmalıdır. Bu sayede Kategori bazlı URL Filtreleme yapabilmelidir. Farklı kullanıcı ve kullanıcı gruplarına farklı kategorilerde URL filtreleme uygulanabilmelidir.</i>	
11.38.	Different URL filtering policies should be set for each firewall rule written on the basis of source (IP and / or user), target, and service.	<i>Kaynak (IP ve/veya kullanıcı) , hedef, servis bazında yazılan her güvenlik duvarı kuralında farklı URL filtreleme politikaları set edilebilmelidir.</i>	
11.39.	At least 75 URL categories on the system and more than 250 million were categorized URL should contain.	<i>Sistem üzerinde en az 75 adet URL kategorisi ve 250 milyondan fazla kategorize edilmiş URL bulunmalıdır.</i>	

11.40.	There should be no user limit for the URL Filtering function of the system and should be offered with an unlimited user license.	<i>Sistemin URL Filtreleme fonksiyonu için kullanıcı sınırı olmamalı ve sınırsız kullanıcı lisansı ile teklif edilmelidir.</i>	
11.41.	Apart from URL filtering categories, the addresses requested as wildcard, regex, or full URL should be defined under different profiles (such as *.gov.tr *). Access to these defined addresses should be blocked or allowed.	<i>URL filtreleme kategorileri dışında, wildcard, regex veya tam URL olarak istenilen adreslerin farklı profiller altında tanımları yapılabilirdir (Örneğin *.gov.tr* gibi). Tanımı yapılan bu adreslere erişim engellenebilmeli veya izin verilebilmelidir.</i>	
11.42.	URL filtering warning screens can be customized.	<i>URL filtreleme uyarı ekranları özelleştirilebilecektir.</i>	
11.43.	All systems offered must have IPv6 support and support dual-stack feature, which allows the use of IPv4 and IPv6 protocols at the same time. At least under IPv6; IPv6 addressing, IPv6 static routing, IPv6 DNS, IPv6 security rules, IPv6 recording and reporting, and Ping6 must be supported. IPS, Application Control, and Web Filtering should be able to be applied to IPv6 traffic.	<i>Teklif edilen tüm sistemlerin IPv6 desteği bulunmalıdır ve IPv4 ile IPv6 protokollerinin aynı anda kullanımına izin veren dual-stack özelliği desteklenmelidir. IPv6 kapsamında en az; IPv6 adresleme, IPv6 statik yönlendirme, IPv6 DNS, IPv6 güvenlik kuralları, IPv6 kayıt ve raporlama ve Ping6 desteklenmelidir. IPv6 trafiğine IPS, Uygulama Denetimi ve Web Filtreleme yapılabilirdir.</i>	
11.44.	System configuration should be able to be done by at least the following methods: • With serial connection, through the console port, • With Http and	<i>Sistem yapılandırması en az aşağıdaki yöntemler ile yapılabilirdir:</i> • <i>Seri bağlantı ile konsol port üzerinden,</i> • <i>Http ve Https bağlantı ile web ara yüz üzerinden veya üreticinin kendisine</i>	

	Https connection, via web interface or via the manufacturer's own Linux or Windows based management application • With SSH connection, via the command line	ait Linux veya Windows tabanlı yönetim uygulaması üzerinden • SSH bağlantı ile komut satırı (command line) üzerinden	
11.45.	Network Firewall The system must support SNMP and must support SNMPv3	Ağ Güvenlik Duvarı Sistemin SNMP desteği olmalı ve SNMPv3 desteklemelidir	
11.46.	Network Firewall System operating system and software updates must be made via the Web interface, TFTP or FTP.	Ağ Güvenlik Duvarı Sistemi işletim sistemi ve yazılım güncellemelerini Web ara yüzü, TFTP veya FTP üzerinden yapılabilmelidir.	
11.47.	Updates of systems running redundantly should be able to be made at least via web gui. Systems should be able to be automatically updated sequentially without disrupting traffic.	Yedekli olarak çalışan sistemlerin güncellemeleri en az web gui üzerinden yapılabilmelidir. Sistemler otomatik olarak, trafiği kesintiye uğratmayacak şekilde sırayla güncellenebilmelidir.	
11.48.	There should be no user limit for the system about the Firewall, VPN, IPS functions and should be offered with an unlimited user license. Licenses to perform Software / operating system updates for 3 years and IPS, Application Recognition and Control, AntiVirus, URL Category Filtering services and	Sistemin; Firewall, VPN, IPS fonksiyonlarının hiç biri için kullanıcı sınırı olmamalıdır ve sınırsız kullanıcı lisansı ile teklif edilmelidir. Ağ Güvenlik Sisteminin 3 yıl süre ile Yazılım/işletim sistemi güncellemelerini ve en az 3 yıl süre için IPS, Uygulama Tanıma ve Kontrolü, AntiVirus, URL Kategori Filtreleme servis ve güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.	

	updates for at least 3 years of the Network Security System must be provided with the system.		
11.49.	The recommended firewall system manufacturer must have one or more of its products, entered the "NSS Labs Network IPS" and "NSS Labs Next Generation Firewall" tests and should be in the recommended product category.	<i>Önerilecek güvenlik duvarı sistemi üreticisinin, bir veya birden fazla ürünü, "NSS Labs Network IPS" ve "NSS Labs Next Generation Firewall" testlerine girmiş ve tavsiye edilen ürün kategorisinde olması gereklidir.</i>	
11.50.	The Firewall System must have a geographic database. It should be able to cut the traffic from the specified country or countries by writing a rule on a country basis.	<i>Güvenlik Duvarı Sisteminin coğrafi veri tabanı bulunmalıdır. Ülke bazında kural yazılarak belirtilen ülke veya ülkelerden gelen trafiği kesebilmelidir.</i>	
11.51.	The proposed security system will also have load balancing features. • It should be able to load balance all sessions based on HTTP, HTTPS, SSL for Layer 7, TCP and UDP for Layer 4, and IP protocol for Layer 3. • IPS, AV policies should be available for servers with load balancing. • For HTTP and HTTPS connections, the source IP address should be able to	<i>Teklif edilen güvenlik sistemi, aynı zamanda yük dengeliyici özelliklerine sahip olacaktır.</i> • <i>Layer 7 için HTTP, HTTPS, SSL, Layer 4 için TCP ve UDP , Layer 3 için IP protokolü bazında tüm oturumlar için yük dengelemesi yapabilmelidir.</i> • <i>Yük dengelemesi uygulanan sunucular için IPS, AV politikaları kullanılabilmelidir.</i> • <i>HTTP, HTTPS bağlantıları için fiziksel sunuculara kaynak IP adresinin gitmesi</i>	

	go to physical servers. • Must have SSL Offloading feature for SSL connections. • Traffic should be able to be distributed to the real servers of the institution by the following methods: • Source IP hash information • Round robin • By making a weight definition in the real server definitions against the possibility of the servers having different powers • The traffic is sent to the first of the active real servers and the load is sent to the next active server in case of inactivity. • Based on	<i>sağlanabilmelidir.</i> • <i>SSL bağlantıları için SSL Offloading özelliği olmalıdır.</i> • <i>Trafik kurum gerçek sunucularına aşağıdaki yöntemlerle dağıtılabilmelidir:</i> • <i>Kaynak Ip hash bilgisi</i> • <i>Round robin</i> • <i>Sunucuların farklı güçlerde olabilme ihtimaline karşı gerçek sunucu tanımlarında ağırlık tanımı yapılarak</i> • <i>Aktif durumda olan gerçek sunuculardan ilkinde trafiğin gönderilip, devre dışı kalması durumunda sonraki aktif sunucuya yükün gönderilmesi</i> • <i>Ping paketlerine verilen cevaplar esas alınması</i> • <i>Sunucular üzerine</i>	
--	--	---	--

	responses to ping packets - Depending on the session number information directed to the servers - During load sharing, it should be able to check server availability by tcp, http (eg checking http://190.1.128.1 / test_page.htm), and ping.	<i>yönlendirilen session sayı bilgisine bağlı olarak</i> <i>Yük paylaşımı sırasında sunucu bulunurluğunu tcp, http (örneğin http://190.1.128.1/test_page.htm adresinin kontrolü ile) ve ping ile kontrol edebilmelidir.</i>	
11.52.	It should be able to perform vulnerability scanning tests on specified systems.	<i>Belirlenen sistemler üzerinde zaafiyet tarama testi yapabilmelidir.</i>	
11.53.	The proposed system can work as a wifi controller, so it can be used for the management of wireless access devices that can be used.	<i>Teklif edilen sistem wifi controller olarak çalışabilecek, bu sayede kullanılacak kablosuz erişim cihazlarının yönetimi için kullanılabilir.</i>	
11.54.	Wan will have optimization features.	<i>Wan optimizasyon özelliklerine sahip olacaktır.</i>	
11.55.	It should be able to optimize the protocol for Common Internet File System (CIFS), FTP, HTTP, MAPI, and TCP sessions.	<i>Common Internet File System (CIFS), FTP, HTTP, MAPI ve TCP oturumları için protokol optimizasyonu yapabilmelidir.</i>	
11.56.	Must have web cache feature.	<i>Web cache özelliği olmalıdır.</i>	

11.57.	It must support Web cache communication Protocol (WCCP).	<i>Web cache communication Protocol (WCCP) desteęi olmalıdır.</i>	
11.58.	Proposed security system should have at least 10/10/6 Gbps Firewall performance value for 1518/512/64 Byte IP packet size in the proposed configuration. These values should be stated in the documentation for the product offered and the manufacturer should have posted these values publicly on his website.	<i>Teklif edilen güvenlik sistemi, teklif edilen konfigürasyonda, 1518/512/64 Byte IP paket büyüklüęü için en az 10/10/6 Gbps Firewall performansı deęerine sahip olmalıdır. Bu deęerler teklif edilen ürün ile ilgili belgelerinde belirtilmiř ve üretici bu deęerleri kendi web sitesinde herkese açık bir şekilde yayınlamıř olmalıdır.</i>	
11.59.	The system must support at least 700 thousand sessions at the same time and must have a performance of at least 35 thousand new sessions per second. These values should be specified in the product documentation offered. These values should be stated in the documentation for the product offered and the manufacturer should have published these values publicly on his website.	<i>Sistem aynı anda en az 700bin oturumu desteklemeli ve saniyede en az 35 Bin yeni oturum açabilme performansına sahip olmalıdır. Bu deęerler teklif edilen ürün belgelerinde belirtilmiř olmalıdır. Bu deęerler teklif edilen ürün ile ilgili belgelerinde belirtilmiř ve üretici bu deęerleri kendi web sitesinde herkese açık bir şekilde yayınlamıř olmalıdır.</i>	
11.60.	Firewall System must have at least 6.5 Gbps IPSec VPN throughput for AES128 + SHA-1 . These values should be stated in the documentation for the product offered and the manufacturer should have published these values publicly on his website.	<i>Güvenlik Duvarı Sisteminin AES128 + SHA-1 için en az 6.5 Gbps IPSec VPN throughput deęerine sahip olmalıdır. Bu deęerler teklif edilen ürün ile ilgili belgelerinde belirtilmiř ve üretici bu deęerleri kendi web sitesinde herkese açık bir şekilde yayınlamıř olmalıdır.</i>	
11.61.	The system must support 200 Site-to-Site and at	<i>Sistem Site-to-Site 200 adet ve Client-to-Site için en az 500</i>	

	least 500 IPSec VPN tunnels for Client-to-Site. The device must be able to work compatible with VPN Gateway devices that comply with the standards that support the aforementioned VPN protocols.	<i>adet IPSec VPN tünelleri desteklemelidir. Cihaz, anılan VPN protokollerini destekleyen standartlarla uyumlu VPN Gateway cihazları ile uyumlu çalışabilmelidir</i>	
11.62.	The system must have a performance rating of 1.4 Gbps IPS throughput. This value should be stated in the documentation for the product offered, and the manufacturer should have posted these values publicly on his website.	<i>Sistem 1.4 Gbps IPS throughput performans değerine sahip olmalıdır. Bu değer teklif edilen ürün ile ilgili belgelerinde belirtilmiş ve üretici bu değerleri kendi web sitesinde herkese açık bir şekilde yayınlamış olmalıdır.</i>	
11.63.	There should be at least 5 10/100/1000 Base-T and 2 Management Port ports on the system.	<i>Sistem üzerinde En az 5 adet 10/100/1000 Base-T, 2 adet Management Port bağlantı noktası olmalıdır.</i>	
11.64.	The system must be able to send records to the Syslog Servers, to the Registration / Reporting System that will be offered with the System, and to keep records.	<i>Sistem Syslog Sunuculara, Sistem ile birlikte teklif edilecek Kayıt/Raporlama Sistemine kayıt gönderebilmeli kayıt tutabilmelidir.</i>	
11.65.	Log and Hotspot software that fully complies with the Law No. 5651 should be offered with the system.	<i>Sistemle birlikte 5651 nolu kanunu tam karşılayan Log ve Hotspot yazılımı teklif edilmelidir.</i>	
11.66.	The proposed system must have a software and hardware warranty of at least 3 years. Licenses to perform Software / Firmware updates for 3 years must be given with the system.	<i>Teklif edilen sistemin en az 3 yıl yazılım ve donanım garantisi bulunmalıdır. 3 yıl süre ile Yazılım/Firmware güncellemelerini yapacak lisanslar sistemle birlikte verilmelidir.</i>	
Item to be supplied description		Tedarik edilecek ürün tanımı	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce</i>

			<i>olarak verilmelidir</i>
12. Personal Computer		<i>Bilgisayar</i>	Brand/Model // <i>Marka/Model:</i>
12.1.	The computer to be offered must be a corporate product. The warranty period should be extended with additional packages.	<i>Teklif edilecek bilgisayar kurumsal ürün olmalıdır. Garanti süresi ek paketler ile uzatılabilmelidir.</i>	
12.2.	The frame size of the computer must be in MFF form.	<i>Bilgisayarın kasa tipi MFF formunda olmalıdır.</i>	
12.3.	The processor of the computer should have a minimum 2.2 GHz base CPU speed.	<i>Bilgisayarın işlemcisi en az 2.2 GHz temel hızında olmalıdır.</i>	
12.4.	The computer's RAM memory must be at least 4GB.	<i>Bilgisayarın RAM hafızası en az 4GB olmalıdır.</i>	
12.5.	The disk capacity of the computer must be at least 500GB.	<i>Bilgisayarın disk kapasitesi en az 500GB olmalıdır.</i>	
12.6.	The operating system of the computer must be Windows 10 Pro or equivalent.	<i>Bilgisayarın işletim sistemi Windows 10 Pro ya da eşdeğeri olmalıdır.</i>	
12.7.	There should be at least 4 USB 3.1 ports and at least 2 USB 2.0 ports on the computer. At least 2 of the USB ports should be located on the front of the case.	<i>Bilgisayarın üzerinde en az 4 adet USB 3.1 portu ve en az 2 adet USB 2.0 portu bulunmalıdır. USB portlarının en az 2 tanesi kasanın ön tarafında konumlandırılmalıdır.</i>	
12.8.	The computer must have at least 1 RJ-45 ethernet port.	<i>Bilgisayarın en az 1 adet RJ-45 ethernet portu bulunmalıdır.</i>	
12.9.	There should be at least 1 HDMI 1.4 and at least 1 DisplayPort 1.2 port on the computer for Monitor connection.	<i>Bilgisayarın üzerinde Monitör bağlantısı için en az 1 adet HDMI 1.4 ve en az 1 adet DisplayPort 1.2 portu bulunmalıdır.</i>	

12.10.	There should be headphone and microphone jacks on the computer.	<i>Bilgisayarın üzerinde kulaklık ve mikrofon girişleri bulunmalıdır.</i>	
12.11.	DVD-RW must be on the computer.	<i>Bilgisayar üzerinde DVD-RW bulunmalıdır.</i>	
12.12.	The computer must have at least 2 M.2 slots.	<i>Bilgisayarın en az 2 adet M.2 yuvası bulunmalıdır.</i>	
12.13.	At least 23.8 "monitor of the same brand should be provided with the computer.	<i>Bilgisayar ile birlikte aynı marka en az 23.8" monitör verilmelidir.</i>	
12.14.	The monitor must support 1920 x 1080 60Hz resolution.	<i>Monitör 1920 x 1080 60Hz çözünürlüğü desteklemelidir.</i>	
12.15.	The brightness of the monitor should be at least 250cd / m2.	<i>Monitör ün parlaklığı en az 250cd/m2 olmalıdır.</i>	
12.16.	The response time of the monitor should be at most 6ms.	<i>Monitör ün tepkime süresi en çok 6ms olmalıdır.</i>	
12.17.	The monitor should have a depth of 16.7 Million colors.	<i>Monitör 16.7 Milyon renk derinliğine sahip olmalıdır.</i>	
12.18.	The monitor should be visible horizontally and vertically at an angle of at least 178 degrees.	<i>Monitör yatayda ve dikeyde en az 178 derecelik açıda görülebilmelidir.</i>	
12.19.	The monitor should be height adjustable.	<i>Monitörün yüksekliği ayarlanabilir olmalıdır.</i>	
12.20.	The monitor must have anti-glare properties.	<i>Monitör parlama önleyici özelliğe sahip olmalıdır.</i>	
12.21.	The same brand of wireless keyboard and wireless mouse should be given with the computer.	<i>Bilgisayar ile birlikte aynı marka kablosuz klavye ve kablosuz Mouse verilmelidir.</i>	
12.22.	The individual computer and monitor must have a warranty period of at least 3 years.	<i>Teklil edilen bilgisayar ve monitör en az 3 yıl garanti süresine sahip olmalıdır.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen</i>

			<i>teknik özellikler İngilizce olarak verilmelidir</i>
13. Data Center Security Software		<i>Veri Merkezi Güvenlik Yazılımı</i>	Brand/Model // Marka/Model:
13.1.	All components that make up the Data Center Security Software to be offered will be a single product from the same manufacturer. Even if it belongs to the same manufacturer, it will not be a solution created by combining different products.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımını oluşturan tüm bileşenler aynı üreticiye ait tek bir ürün olacaktır. Aynı üreticiye dahi ait olsa farklı ürünlerin bir araya getirilmesinden oluşturulan bir çözüm olmayacaktır.</i>	
13.2.	The Data Center Security Software to be offered will be capable of managing the security policies of server systems in physical, virtual, and cloud environments from a single point.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı fiziksel, sanal ve bulut ortamdaki sunucu sistemlerin güvenlik politikalarını tek bir noktadan yönetebilecek özellikte olacaktır.</i>	
13.3.	The Data Center Security Software to be offered should be offered to license 10 servers.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı 10 adet sunucuyu lisanslayacak şekilde teklif edilmelidir.</i>	
13.4.	The Data Center Security Software to be offered will consist of Central Management System and Operating system agent applications.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi ve İşletim sistemi ajan uygulamalarından oluşacaktır.</i>	
13.5.	The Data Center Security Software to be offered will be able to run on the following operating system platforms: - Windows Server 2016 (64-bit) - Windows Server 2012 or 2012 R2 (64-bit) — Full Server or Server Core - Windows Server	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı aşağıdaki işletim sistemi platformlarında çalışabilecektir:</i> - Windows Server 2016 (64-bit) - Windows Server 2012 or 2012 R2 (64-bit) — Full Server ya da Server Core - Windows Server 2008 R2 (64-bit)	

	2008 R2 (64-bit) • Windows Server 2008 (32-bit and 64-bit) • Windows Server 2003 SP2 or higher (32-bit and 64-bit) • Windows 10 or 10 TH2 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows 8 (32-bit and 64-bit) • Windows 7 (32-bit and 64-bit) • Windows XP (32-bit and 64-bit) • Hyper-V on Windows 2012 R2, 2012, 2008 R2, 8, and 8.1 • Red Hat Enterprise Linux 7 (32-bit and 64-bit) • Red Hat Enterprise Linux 6 (32-bit and 64-bit) • Red Hat Enterprise Linux 5 (32-bit and 64-bit) • CentOS 7 (32-bit and 64-bit) • CentOS 6 (32-bit and 64-bit) • CentOS 5 (32-bit and 64-bit) • Oracle Linux 7 (32-bit and 64-bit) • Oracle Linux 6 (32-bit and 64-bit) • Oracle Linux 5 (32-bit and 64-bit) • SUSE Enterprise Linux 12 (64-bit) • SUSE Enterprise Linux 11 SP1, SP2, and SP3 (32-bit and 64-bit) • CloudLinux 7 (32-bit and 64-bit) • CloudLinux 6 (32-bit and 64-bit) • Debian 7 (64-bit)	• <i>Windows Server 2008 (32-bit ve 64-bit)</i> • <i>Windows Server 2003 SP2 ya da daha yükseği (32-bit ve 64-bit)</i> • <i>Windows 10 or 10 TH2 (32-bit ve 64-bit)</i> • <i>Windows 8.1 (32-bit ve 64-bit)</i> • <i>Windows 8 (32-bit ve 64-bit)</i> • <i>Windows 7 (32-bit ve 64-bit)</i> • <i>Windows XP (32-bit ve 64-bit)</i> • <i>Hyper-V on Windows 2012 R2, 2012, 2008 R2, 8, ve 8.1</i> • <i>Red Hat Enterprise Linux 7 (32-bit ve 64-bit)</i> • <i>Red Hat Enterprise Linux 6 (32-bit ve 64-bit)</i> • <i>Red Hat Enterprise Linux 5 (32-bit ve 64-bit)</i> • <i>CentOS 7 (32-bit ve 64-bit)</i> • <i>CentOS 6 (32-bit ve 64-bit)</i> • <i>CentOS 5 (32-bit ve 64-bit)</i> • <i>Oracle Linux 7 (32-bit ve 64-bit)</i> • <i>Oracle Linux 6 (32-bit ve 64-bit)</i> • <i>Oracle Linux 5 (32-bit ve 64-bit)</i> • <i>SUSE Enterprise Linux 12 (64-bit)</i> • <i>SUSE Enterprise Linux 11 SP1, SP2, ve SP3 (32-bit and 64-bit)</i> • <i>CloudLinux 7 (32-bit ve 64-bit)</i> • <i>CloudLinux 6 (32-bit ve 64-bit)</i> • <i>Debian 7 (64-bit)</i> • <i>Debian 8 (64-bit)</i>	
--	--	---	--

	• Debian 8 (64-bit) • Ubuntu 16.04 LTS (64-bit) • Ubuntu 14.04 LTS (64-bit) • Solaris 11, 11.2, or 11.3 (64-bit, SPARC, or x86) • Solaris 10 Update 11 (64-bit, SPARC, or x86)	• Ubuntu 16.04 LTS (64-bit) • Ubuntu 14.04 LTS (64-bit) • Solaris 11, 11.2, or 11.3 (64-bit, SPARC, ya da x86) • Solaris 10 Update 11 (64-bit, SPARC, ya da x86)	
13.6.	The Data Center Security Software to be offered should support working in a highly accessible architecture.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı yüksek erişilebilir mimaride çalışmayı desteklemelidir.</i>	
13.7.	The Data Center Security Software Central Management System to be proposed must support working on the following operating systems: • Windows Server 2016 (64-bit) • Windows Server 2012 (64-bit) • Windows Server 2012 R2 (64-bit) • Red Hat Enterprise Linux 7 (64-bit)	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi aşağıdaki işletim sistemleri üzerinde çalışmayı desteklemelidir:</i> • Windows Server 2016 (64-Bit) • Windows Server 2012 (64-Bit) • Windows Server 2012 R2 (64-Bit) • Red Hat Enterprise Linux 7 (64-Bit)	
13.8.	The Data Center Security Software to be proposed should support working with the following systems as the Central Management System database. • Oracle Database 12c, • Microsoft SQL Server 2016 • Microsoft SQL Server 2014, • Microsoft SQL Server 2012, • Postgre SQL 9.6 (Core Distribution & Amazon	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı Merkezi Yönetim Sistemi veritabanı olarak aşağıdaki sistemler ile çalışmayı desteklemelidir.</i> <i>Oracle Database 12c, Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, Postgre SQL 9.6 (Core Distribution & Amazon RDS) ya da Oracle RDS</i>	

	RDS) • Microsoft SQL RDS or Oracle RDS		
13.9.	On the Data Center Security Software to be offered, there will be intrusion detection and prevention, firewall, malware prevention, website reliability, integrity monitoring, log inspection, and application control components, and all components related to these functions will be offered.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde saldırı tespit ve önleme, güvenlik duvarı, zararlı yazılım önleme, web sitesi güvenilirliği, bütünlük gözleme, kütük inceleme ve uygulama kontrolü bileşenleri bulunacak, bu işlevlerle ilgili tüm bileşenler teklif edilecektir.</i>	
13.10.	The attack detection and prevention component to be found on the Data Center Security Software to be proposed will be in an architecture that can scan incoming and outgoing traffic and work with deep packet inspection (DPI).	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak saldırı tespit ve önleme bileşeni gelen ve giden trafiği tarayabilecek ve derin paket inceleme (DPI) çalışabilecek mimaride olacaktır.</i>	
13.11.	Virtual Patch functionality on Windows systems will be supported by the intrusion detection and prevention module that will serve on the proposed Data Center Security Software . When necessary, modules provided at network level can be switched to "monitoring" mode.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde hizmet verecek olan saldırı tespit ve önleme modülü marifeti ile Windows sistemler üzerinde Sanal Yama işlevi desteklenecektir. Gerekli durumlarda ağ seviyesinde sağlanan modüller "izleme" moduna alınabilecektir.</i>	
13.12.	The Data Center Security Software to be offered will include the virtual patch (host based IPS) feature. With the virtual patch feature, network vulnerabilities on the servers can be detected, and they can be turned off manually or automatically,	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı, sanal yama (host based IPS) özelliğini barındıracaktır. Sanal yama özelliği ile sunucular üzerinde bulunan ağ zafiyetleri tespit edilebilecek, isteğe bağlı olarak manuel veya otomatik olarak kapatılabilecektir.</i>	

	optionally.		
13.13.	The firewall component to be found on the Data Center Security Software to be proposed must be capable of preventing denial of service attacks (DoS) and discovery scans.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak olan güvenlik duvarı bileşeni hizmet dışı bırakma saldırılarını (DoS) ve keşif taramalarını engelleme yeteneğine sahip olmalıdır.</i>	
13.14.	Integrity monitoring component to be found on the proposed Data Center Security Software will be able to monitor and report changes in critical operating system files, directories, registry keys, and values in real-time and generate alarms.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak bütünlük gözleme bileşeni kritik işletim sistemi dosyaları, izinleri, kayıt defteri (registry) anahtar ve değerlerindeki değişiklikleri gerçek zamanlı izleyerek rapor edebilecek, alarm üretebilecektir.</i>	
13.15.	The log analysis component to be found on the Data Center Security Software to be proposed will be able to monitor the log records and logs of the operating system and applications on the operating system it is running on, and report suspicious situations and generate alarms.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üzerinde bulunacak kütük inceleme bileşeni çalıştığı işletim sistemi üzerindeki işletim sistemi ve uygulamalara ait günlük kayıtları ve kütükleri izleyerek şüpheli durumları rapor edebilecek, alarm üretebilecektir.</i>	
13.16.	The Data Center Security Software to be offered will be able to access the manufacturer's Global Threat Intelligence service, and with this service, it will be able to make reputation inquiries for web pages, electronic mail resources, and files.	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı üreticinin Global Tehdit İstihbarat hizmetine erişebilecek, bu hizmet sayesinde web sayfaları, elektronik posta kaynakları ve dosyalar için saygınlık sorguları yapabilecektir.</i>	
13.17.	The Data Center Security Software to be offered will support integration with the same manufacturer's Detailed Analysis System for Advanced Attacks. With	<i>Teklif edilecek Veri Merkezi Güvenlik Yazılımı, aynı üreticinin Gelişmiş Saldırıları İçin Detaylı Analiz Sistemi ile entegrasyonu destekleyecektir. Bu</i>	

	this integration, they will be able to send suspicious files for analysis. It will also be able to block files and URLs found as a result of the analysis.	<i>entegrasyon ile şüpheli gördüğü dosyaları analize gönderebilecektir. Ayrıca analiz sonucu bulunan dosya ve URL leri bloklayabilecektir.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
14. User Security Solution		<i>Kullanıcı Güvenliği Çözümü</i>	Brand/Model // Marka/Model:
14.1.	All components to be offered will belong to the same manufacturer.	<i>Teklif edilecek tüm bileşenler aynı üreticiye ait olacaktır.</i>	
14.2.	The "User Security" solution to be offered will be offered for at least 15 end users.	<i>Teklif edilecek "Kullanıcı Güvenliği" çözümü en az 15 son kullanıcı için teklif edilecektir.</i>	
14.3.	The Anti-malware Software to be offered must support the endpoint platforms listed below. • Windows 7 SP1 • Windows 8.1 • Windows 10 • Windows Server 2008R2 (64bit) • Windows Server 2012 (64bit) • Windows Server 2012R2 (64bit) • Windows Server 2016 (64bit) • Windows Server 2019 (64bit)	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aşağıda listelenen uç nokta platformlarını desteklemelidir.</i> • Windows 7 SP1 • Windows 8.1 • Windows 10 • Windows Server 2008R2 (64bit) • Windows Server 2012 (64bit) • Windows Server 2012R2 (64bit) • Windows Server 2016 (64bit) • Windows Server 2019 (64bit)	
14.4.	The Anti-malware to be offered should support the database platforms listed below. • Microsoft SQL Server	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aşağıda listelenen veritabanı platformlarını desteklemektedir.</i>	

	2008 Express SP2 • Microsoft SQL Server 2008 • Microsoft SQL Server 2008R2 • Microsoft SQL Server 2012 • Microsoft SQL Server 2014 • Microsoft SQL Server 2016 Express SP1 • Microsoft SQL Server 2016 • Microsoft SQL Server 2016 SP1 • Microsoft SQL Server 2016 SP2 • Microsoft SQL Server 2017	• <i>Microsoft SQL Server 2008 Express SP2</i> • <i>Microsoft SQL Server 2008</i> • <i>Microsoft SQL Server 2008R2</i> • <i>Microsoft SQL Server 2012</i> • <i>Microsoft SQL Server 2014</i> • <i>Microsoft SQL Server 2016 Express SP1</i> • <i>Microsoft SQL Server 2016</i> • <i>Microsoft SQL Server 2016 SP1</i> • <i>Microsoft SQL Server 2016 SP2</i> • <i>Microsoft SQL Server 2017</i>	
14.5.	The Anti-malware Management server to be offered must be accessed and managed through the Web interface.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim sunucusuna Web ara yüzünden erişilmeli ve yönetim sağlanabilmelidir.</i>	
14.6.	The communication between the Malware Prevention Software management server to be offered and the agent software to run on the end user systems must be encrypted in the AES-256 encryption standard.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim sunucusu ile son kullanıcı sistemler üzerinde çalışacak ajan yazılımı arasındaki iletişim AES-256 şifreleme standardında şifreli olarak gerçekleştirilebilmelidir.</i>	
14.7.	The anti-malware software to be offered must be able to fully protect the operating systems on which it works against viruses, trojans, worms, and spyware, and must be able to provide full protection against malicious codes spreading	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde çalıştığı işletim sistemlerini virüs, truva atı, worm ve spyware lere karşı tam olarak koruyabilmeli ve network üzerinden yayılan zararlı kodlara karşıda tam koruma sağlayabilmelidir.</i>	

	over the network.		
14.8.	The Malware Prevention Software to be offered will monitor the suspicious file encryption activities of such malicious software on client systems in order to detect ransomware type malware and will be able to stop these encryption activities by quarantining or terminating them.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ransomware türünde zararlı yazılımları tespit etmek üzere, bu tip zararlı yazılımların istemci sistemler üzerindeki şüpheli dosya şifreleme faaliyetlerini izleyecek ve bu şifreleme faaliyetlerini karantinaya alarak ya da sonlandırarak durdurabilecektir.</i>	
14.9.	The Malware Prevention Software to be offered will be able to work with predictive machine learning method and detect malicious software without the need for virus signatures.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı öngörüs el makine öğrenme yöntemi ile çalışabilecek, virüs imzalarına ihtiyaç duymadan zararlı yazılımları tespit edebilecektir.</i>	
14.10.	The Anti-malware Software to be offered should be able to provide kernel-level protection against rootkits.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı rootkitlere karşı kernel seviyesinde koruma sağlayabilmelidir.</i>	
14.11.	The Malware Prevention Software to be offered should provide a website rating service that will provide desktop level protection against web threats. With this feature, users should warn and block access before accessing web pages with harmful content.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı web tehditlerine karşı desktop seviyesinde koruma sağlayacak olan web sitesi derecelendirme hizmet alabilmesini sağlamalıdır. Bu özellik ile kullanıcıların, zararlı içerikli olan web sayfalarına erişmeden önce uyarmalı ve erişim engellemesi sağlamalıdır.</i>	
14.12.	In addition to malicious content sites that are blocked by the proposed Anti-Malware website rating feature, system administrators should be able to create their own allowed and banned lists.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı web sitesi derecelendirme özelliğinin engellediğ i zararlı içerikli sitelere ek olarak, sistem yöneticileri, kendi izinli ve yasaklı listelerini oluşturabilmelidir.</i>	

14.13.	The Malware Prevention Software to be offered should contain signatures and algorithms that can detect malicious codes, especially with different compression methods.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı özellikle farklı sıkıştırma metotları ile kendini içine saklayan zararlı kodları tespit edebilecek imzaları ve algoritmaları içerisinde barındırmalıdır.</i>	
14.14.	The Anti-malware Software to be offered must include a stateful firewall.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı stateful özellikli bir güvenlik duvarı barındırmalıdır.</i>	
14.15.	The firewall on the Anti-malware to be offered should protect against DoS attacks and Syn Flood attacks.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan güvenlik duvarı, DoS ataklarına, Syn Flood ataklarına karşı koruma sağlamalıdır.</i>	
14.16.	All settings made on the proposed Anti-Malware Software should be backed up by the central management software and easily recycled from the previously purchased backup when necessary.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde yapılan tüm ayarlar merkezi yönetim yazılımı yolu ile yedeklenebilmeli ve gerektiğinde kolayca daha önce alınmış yedekten geri döndürülebilmelidir.</i>	
14.17.	With the Malware Prevention Software to be offered, in case of a virus epidemic, shares and port access on the network should be closed with rules to be sent manually. Write rights on the file and folder should be able to be turned off.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile herhangi bir virüs salgını durumunda ağ üzerindeki paylaşımlar ve port erişimleri el ile yollanacak kurallarla kapatılabilmelidir. Dosya ve klasör üzerindeki yazma hakları kapatılabilmelidir.</i>	
14.18.	With the Anti-malware Software to be offered, all virus, spyware and software updates should be done centrally and can be sent to clients remotely, automatically and manually.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile tüm virüs, spyware ve yazılım güncellemeleri merkezi olarak yapılmalı ve istemcilere uzaktan otomatik ve el ile yollanabilmelidir.</i>	
14.19.	The Malware Prevention Software to be offered should have the	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı merkezi sunucunun internet bağlantısı</i>	

	infrastructure to ensure that the manually downloaded update files are applied to the central server even if the central server does not have an internet connection.	<i>olmasa dahi el ile indirilen güncelleme dosyalarının merkezi sunucuya uygulanmasını sağlayacak alt yapıya sahip olmalıdır.</i>	
14.20.	Anti-malware to be offered, mobile users should be able to keep their software under protection with their roaming profile when they are not connected to the center. At the same time, these users should be able to make updates via their internet connection without the need for central management software.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı mobil kullanıcılar merkez ile bağlantıları olmadığı zamanlarda gezici profili ile yazılımları koruma altında olmaya devam edebilmelilerdir. Aynı zamanda bu kullanıcılar merkezi yönetim yazılımına gerek kalmadan bulundukları internet bağlantısı yoluyla güncellemelerini yapabilmelilerdir.</i>	
14.21.	With the Anti-malware to be offered, POP3 e-mail connections should also be able to be checked for malware.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile POP3 e-posta bağlantıları da zararlı yazılımlara karşı denetlenebilmelidir.</i>	
14.22.	The Anti-malware Software to be offered should constantly monitor the activity on the computer whenever a file is opened or run, whenever any changes are made to the file (such as renaming, storing, moving, or copying to a directory or a directory) by looking at the virus signature definitions.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı bilgisayar üzerindeki aktiviteyi herhangi bir dosya açıldığında veya çalıştırıldığında, dosyada herhangi bir değişiklik yapıldığında (yeniden isimlendirme, saklama, taşıma veya bir dizine veya bir dizinden kopyalama gibi) virüs imza tanımlarına bakarak devamlı gözlemlemelidir.</i>	
14.23.	Anti-malware to be offered, the user will be able to scan for viruses on usb disk, hard disk, CDROM, and network drives.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcı usb disk, hard disk, CDROM ve ağ sürücülerinde virüs taraması yapabilecektir.</i>	
14.24.	Anti-malware to be offered will provide external device usage policies for	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcılar için harici aygıt kullanım</i>	

	users. There will be authorization rules for users to authorize the use of external devices.	<i>politikaları sağlayacaktır. Kullanıcılar için harici aygıt kullanım yetkilendirilmesini sağlayan yetki kuralları mevcut olacaktır.</i>	
14.25.	The Anti-malware Prevention Software to be offered will have heuristic scan feature. In this way, files that do not have a signature but are suspected of being viruses can be blocked.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı sezgisel tarama (heuristic scan) özelliğine sahip olacaktır. Bu sayede imzası bulunmayan ancak virüs olmasından şüphelenilen dosyalar bloklanabilecektir.</i>	
14.26.	The Anti-malware Software to be offered will also check for viruses in compressed (zip, etc.) files.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı sıkıştırılmış (zip vb.) dosyalarda da virüs denetimi yapacaktır.</i>	
14.27.	The Anti-malware Software to be offered should support the definition of exception rules so that the desired files and folders are not scanned during scans.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı taramalar sırasında istenilen dosya ve klasörlerin taranmaması için istisna kurallarının tanımlanmasını desteklemelidir.</i>	
14.28.	The Malware Prevention Software to be offered should be able to alert the system administrator via e-mail if the threshold value determined in any virus outbreak or malicious code attacks on the network is exceeded.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı herhangi bir virüs salgını ya da ağ üzerinde yaşanan zararlı kod saldırılarında belirlenen eşik değeri geçilmesi durumunda sistem yöneticisini e-posta yoluyla uyaramelidir.</i>	
14.29.	The Anti-malware to be offered should provide flexibility in processor (CPU) usage during security scans, and include maximum usage level settings.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı güvenlik taramaları sırasında işlemci (CPU) kullanımı konusunda esneklik sağlamalı, maksimum kullanım düzeyi ayarlarını içerisinde barındırmalıdır.</i>	
14.30.	Anti-Malware user components to be offered must be able to be installed via MSI packages. MSI packages should be able to be modified and	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcı bileşenleri MSI paketleri yoluyla kurulabilmelidir. MSI paketleri değiştirilebilmeli ve kurulum seçenekleri ile</i>	

	recreated with installation options.	<i>yeniden yaratılabilmelidir.</i>	
14.31.	The Malware Prevention Software to be offered should support the installations of operating systems from the image.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile imajdan işletim sistemleri kurulumlarını desteklenmelidir.</i>	
14.32.	The Anti-malware Software to be offered should support the reverting to previous versions of the virus update file and the malware scanning engine, both on the client and server side, in case of any problem. (Rollback)	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı herhangi bir sorun anında virüs güncelleme dosyasının ve zararlı tarama motorunun hem istemci hem de sunucu tarafında, bir önceki eski sürümlerine geri dönülmesini desteklemelidir. (Rollback)</i>	
14.33.	Virus, system update, event log, instant virus scanning, etc. on the Anti-malware Management software to be offered. Event records of information should be kept. The storage duration of the event logs on the management software should be determined by the system administrator.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı yönetim yazılımı üzerinde virüs, sistem güncelleme, olay günlüğü, anlık virüs tarama vb. bilgilere ait olay kayıtları tutulmalıdır. Yönetim yazılımı üzerinde olay kayıtlarının saklanma süresi, sistem yöneticisi tarafından belirlenebilmelidir.</i>	
14.34.	The Anti-malware Prevention Software to be offered will be automatically deleted from the system if inactive clients are detected within the specified day-out period.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı zaman aralığı verilerek belirlenen gün aşımında aktif olmayan istemciler tespit edildiği takdirde otomatik olarak sistemden silinmesi sağlanacaktır.</i>	
14.35.	The Anti-malware to be offered should be able to alert the system administrator via e-mail and SNMP as soon as they are found malicious on clients .	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı, istemciler üzerinde zararlı bulunduğu anda e-posta ve SNMP yoluyla sistem yöneticisini uyarabilmelidir.</i>	
14.36.	It should be possible to specify how long the logs	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde</i>	

	will remain in the system on the Anti-malware Prevention Software to be offered, and optimize the log records by defining the automatic deletion process.	<i>üretilecek logların sistemde ne kadar süre kalacağı belirtilebilmeli ve otomatik silme işlemi tanımlanarak log kayıtları üzerinde optimizasyon sağlanabilmelidir.</i>	
14.37.	With the Malware Prevention Software to be offered, the management features of the software to be installed on the clients can be customized by the system administrator through the central management software. The removal of the software from memory should be prevented, and its removal from the system by uninstall should be secured with password protection. The system administrator should be able to block access to the folders where the client software is installed, as well as to deny access within the registry.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile istemcilere yüklenecek yazılımların yönetim özellikleri merkezi yönetim yazılımı yoluyla sistem yöneticisi tarafından özelleştirilebilecektir. Yazılımın hafızadan çıkarılması engellenebilmeli, uninstall ile sistemden kaldırılması şifre korumalı olarak güvenlik altına alınabilmelidir. Sistem yöneticisi isterse istemci yazılımının kurulduğu klasörlere erişimleri engelleyebileceği gibi kayıt defteri içindeki erişimlerini de kesebilmelidir.</i>	
14.38.	Malware Prevention Software to be requested from the list of Spyware and Grayware should be considered as harmless and separated.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı Spyware ve Grayware listesinden istenilen yazılımlar zararsız olarak kabul edilip ayrıştırılabilmelidir.</i>	
14.39.	The Anti-malware Software to be offered must support receiving updates via proxy.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı proxy üzerinden güncellemeleri almayı desteklemelidir.</i>	
14.40.	Support the remote removal of agents located on endpoints with the Anti-malware Software to be offered.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile uç noktalar üzerinden bulunan ajanların uzaktan kaldırılmasını desteklemelidir.</i>	
14.41.	The infected files quarantined with the Anti-malware Prevention Software to be offered	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile karantinaya alınan virüslü dosyalar şifrelenerek</i>	

	should be encrypted and stored.	<i>saklanmalıdır.</i>	
14.42.	More than one update source for the Anti-malware Software to be offered must be defined within the network. For this, an end-user computer with Malware Prevention Software agent installed on it should be used, and a separate computer should not be required for this feature.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı için birden fazla güncelleme kaynağı ağ içinde tanımlanabilmelidir. Bunun için üzerinde Zararlı Yazılım Önleme Yazılımı ajanı yüklü bir son kullanıcı bilgisayarı kullanılabilmesi, bu özellik için ayrı bir bilgisayar ihtiyacı olmamalıdır.</i>	
14.43.	Anti-malware to be offered should be integrated into the central product management software of the same manufacturer as required.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı gerektiğinde aynı üreticinin merkezi ürün yönetim yazılımına entegre olmalıdır.</i>	
14.44.	17.44. The Malware Prevention Software to be offered should be able to start time-dependent and instant scans on clients and monitor their results through the central management software.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı merkezi yönetim yazılımı yoluyla istemciler üzerinde zamana bağlı ve anlık taramalar başlatılıp sonuçları izlenebilmelidir.</i>	
14.45.	The Anti-malware Software to be offered should scan the entire network from a single point, detect clients with and without antivirus software installed, and support the installation of an antivirus agent on clients that are not installed.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı tek noktadan tüm ağı tarayarak antivirüs yazılımı kurulu olan ve olmayan istemcileri tespit etmeli, kurulu olmayan istemcilere antivirüs ajanının kurulmasını desteklemelidir.</i>	
14.46.	The Malware Prevention Software to be offered should support the monitoring method such as changing the system registry keys, changing the host file, installing a new service, and changing	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı istemci üzerinde çalıştırılacak olan yazılımların sistem üzerinde yapacakları değişiklikleri izleyerek daha önceden belirlenecek politikalar dahilinde sistem kayıt defteri</i>	

	existing services within the pre-determined policies by monitoring the changes made by the software that can be run on the client, and these monitoring settings should be edited separately for a specific group or a single client.	<i>anahtarlarının değiştirilmesi, host dosyasının değiştirilmesi, yeni bir servis yüklenmesi ve var olan servislerin değiştirilmesi gibi izleme metodunu desteklemeli ve bu izleme ayarları tüm sistem, belirli bir grup veya tek bir istemci için ayrı ayrı düzenlenebilmelidir.</i>	
14.47.	The Malware Prevention Software to be offered will be able to receive malicious URL, Domain, IP, and Hash information detected by the Detailed Analysis System for Advanced Attacks belonging to the same manufacturer as an update and share it with clients.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırıları İçin Detaylı Analiz Sistemi tarafından tespit edilen zararlı URL, Domain, IP ve Hash bilgisi güncelleme olarak alabilecek ve istemciler ile paylaşabilecektir.</i>	
14.48.	The Malware Prevention Software to be offered will be able to receive the SHA-1 control summary information of the malicious software detected by the Detailed Analysis System for Advanced Attacks belonging to the same manufacturer as an update over the Security Management Software, and will be able to clean these malicious software through the infected clients.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırıları İçin Detaylı Analiz Sistemi tarafından tespit edilen zararlı yazılımların, şüpheli dosyaların SHA-1 kontrol özeti bilgilerini Güvenlik Yönetim Yazılımı üzerinden güncelleme olarak alabilecek ve bu zararlı yazılımları, şüpheli dosyaları bulaştığı istemciler üzerinden temizleyebilecektir.</i>	
14.49.	The Malware Prevention Software to be offered will be able to send suspicious files extracted from USB, e-mail and web pages to the Detailed Analysis System for Advanced Attacks of the same manufacturer, regardless	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı aynı üreticiye ait Gelişmiş Saldırıları İçin Detaylı Analiz Sistemi'ne istemcinin kurum içinde ya da kurum dışında olmasından bağımsız olarak USB, e-posta ve web sayfalarından çekilmiş olan şüpheli dosyaları detaylı</i>	

	of whether the client is in or out of the institution, for detailed analysis.	<i>analiz amacı ile gönderebilecektir.</i>	
14.50.	Proposed Anti-Malware Software will be able to transmit event logs to a SIEM solution via syslog.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı olay kayıtlarını syslog aracılığıyla bir SIEM çözümüne iletebilecektir.</i>	
14.51.	Different administrator roles should be defined on the Anti-malware Prevention Software to be offered, and these users should be able to be pulled from Active Directory if desired.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde farklı yönetici rolleri tanımlanabilmeli ve bu kullanıcılar istenilirse Active Directory üzerinden çekilip kullanılabilir.</i>	
14.52.	The Malware Prevention Software to be offered should be able to quickly generate detailed reports of the connected security software with ready report templates.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı hazır rapor şablonları ile hızlı bir şekilde bağlı bulunan güvenlik yazılımlarına ait detaylı raporlar üretebilmelidir.</i>	
14.53.	Anti-malware to be offered will provide external device usage policies for users. There will be authorization rules for users to authorize the use of external devices.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı kullanıcılar için harici aygıt kullanım politikaları sağlayacaktır. Kullanıcılar için harici aygıt kullanım yetkilendirilmesini sağlayan yetki kuralları mevcut olacaktır.</i>	
14.54.	Special reports will be provided in the Anti-malware Prevention Software to be offered.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında özel raporlar alınması sağlanacaktır.</i>	
14.55.	The Malware Prevention Software to be offered will be able to generate reports in pdf, docx , xlsx formats.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı pdf,docx,xlsx formatlarında rapor üretebilecektir.</i>	
14.56.	Reports created with the Anti-malware Prevention Software to be offered should be able to be generated automatically depending on time.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı ile oluşturulan raporlar zamana bağlı olarak otomatik üretilmelidir.</i>	

14.57.	The Malware Prevention Software to be offered should be able to transmit the automatically generated reports to predetermined people by e-mail.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı otomatik oluşturulan raporları e-posta ile daha önceden belirlenmiş kişilere iletebilmelidir.</i>	
14.58.	The Anti-malware Software to be offered must have integrated data loss prevention (DLP) capability. • The data loss prevention system on the Anti-malware to be offered should have predefined data identifiers and templates and allow the identification of organization-specific identifiers and templates. • The data loss prevention system on the proposed Anti-Malware Software should be able to control access to certain applications and file types by default, and	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı bütünleşmiş veri kaybı önleme özelliğine (DLP) sahip olmalıdır.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi ön tanımlı veri belirleyicileri ve şablonlara sahip olmalı ve kuruma özel belirleyici ve şablonların tanımlanmasına olanak tanımalıdır.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi ön tanımlı olarak belirli uygulama ve dosya tiplerine erişimi denetleyebilmeli, bu işlemi dosya uzantısı tipinden bağımsız olarak gerçek dosya</i>	

	should be able to do this by recognizing the actual file type regardless of the file extension type. It should allow specific definitions for the institution to be made when necessary. • There must be a device control feature on the data loss prevention system on the Anti-malware Prevention Software to be offered. With this feature, data traveling from the client to different devices should be blocked, allowed or recorded according to the rules applied. • The data loss prevention system on the Anti-	<i>tipini tanıyarak yapabilmelidir.</i> <i>Gerektiğinde kuruma özel tanımlamaların yapılmasına olanak sağlamalıdır.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi üzerinde cihaz kontrol özelliği bulunmalıdır. Bu özellik ile istemciden farklı cihazlara doğru giden veriler uygulanan kurallara göre engellenebilmeli, izin verilebilmeli ya da kayıt altına alınabilmelidir.</i> • <i>Teklif edilecek Zararlı Yazılım Önleme Yazılımı üzerinde bulunan veri kaybı önleme sistemi aşağıda belirtilen veri çıkış kanallarını desteklemelidir.</i> • <i>Email Clients</i> • <i>FTP</i> • <i>HTTP ve HTTPS</i>	
--	--	--	--

	malware Prevention Software to be offered must support the following data output channels. • Email Clients • FTP • HTTP and HTTPS • Instant communication applications (Instant Messaging) • SMB protocol • Webmail • Cloud storage services • CD / DVD • P2P applications • PGP encryption • Printer • External data storage • ActiveSync • Windows Clipboard	• Anlık haberleşme uygulamaları (Instant Messaging) • SMB protokolü • Webmail • Bulut depolama servisleri • CD/DVD • P2P uygulamaları • PGP şifreleme • Printer • Harici veri depolama • ActiveSync • Windows Clipboard	
14.59.	The Malware Prevention Software to be offered will have an intrusion detection and prevention feature (HIPS) and a virtual patching feature against zero-day attacks.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında saldırı tespit ve engelleme özelliği (HIPS) ve sıfırcı gün ataklarına karşı sanal yama yapma özelliği bulunacaktır.</i>	
14.60.	The Anti-malware to be offered will have an application control feature:	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında uygulama kontrolü özelliği bulunacaktır:</i>	
14.61.	With the "lockdown" feature in the application control in the Malware Prevention Software to be offered, it will be able to learn the user's current	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde "lockdown" özelliği ile kullanıcının mevcut envanterini öğrenip sadece</i>	

	inventory and only allow them to prevent new applications from running.	<i>onlara izin vererek, yeni uygulamaların çalışmasını engelleyebilecektir.</i>	
14.62.	Whitelist-blacklist rules can be created in the application control in the Anti-malware Prevention Software to be offered.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde whitelist-blacklist kurallar oluşturulabilecektir.</i>	
14.63.	In the application control in the Malware Prevention Software to be offered, blocking / allowing rules can be written according to the HASH information of the applications.	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolünde uygulamaların HASH bilgilerine göre bloklama/izin verme kurallar yazılabilecektir.</i>	
14.64.	The application control included in the Anti-malware Prevention Software to be offered can only work in logging mode	<i>Teklif edilecek Zararlı Yazılım Önleme Yazılımında bulunan uygulama kontrolü sadece loglama modunda çalışabilecektir.</i>	
Item to be supplied description		<i>Tedarik edilecek ürün tanımı</i>	Offered technical specifications by the Bidder shall be inserted in English <i>Firma tarafından teklif edilen teknik özellikler İngilizce olarak verilmelidir</i>
15. Uninterruptable Power Supply		<i>Kesintisiz Güç Kaynağı</i>	Brand/Model // <i>Marka/Model:</i>
15.1.	Bidding manufacturers must certify that they have the international ISO 9001-14001 and CE standard.	<i>Teklif veren üretici kuruluşlar Uluslararası ISO 9001-14001 ve CE standardına sahip olduklarını belgelemelidirler.</i>	
15.2.	In order not to affect computers and sensitive electronic systems, it must comply with the EN 62040-2 (EMC) standard, which minimizes electromagnetic effects, and the EN 62040-1 standard, which includes safety items.	<i>Bilgisayar ve hassas elektronik sistemlerin etkilenmemesi bakımından, elektromanyetik etkileri minimuma indiren EN 62040-2 (EMC) standardına ve güvenlik maddelerini içeren EN 62040-1 standardına uygun olmalıdır</i>	
15.3.	The offered product	<i>Teklif edilen ürün</i>	

	should be available in tower type and rack type when desired.	<i>istenildiğinde tower tip, istenildiğinde ise rack tipi kullanılabilirdir.</i>	
15.4.	The company must provide the user manual and the service manual for maintenance and repair, written in Turkish language, free of charge, at the time of delivery of the UPSs, separately for each UPS.	<i>Firma KGK' ların teslimi anında, herbir KGK için ayrı ayrı olmak üzere, kullanıcı el kitabını ve bakım onarım için servis el kitabını, Türkçe dilinde matbaa harfleriyle yazılmış halde ücretsiz olarak vermelidir.</i>	
15.5.	The UPSs will be an original model of the manufacturer's mass production. There will be no broken, cracked, scratched, paint defect, or deformed parts and will not be used.	<i>KGK 'lar imalatçının orijinal seri imalatı bir model olacaktırKırık, çatlak, çizik, boya hatası ve deformasyona uğramış hiçbir parçası bulunmayacak, kullanılmış olmayacaktır.</i>	
15.6.	State-of-the-art materials and elements should be used in the manufacture of UPSs.	<i>KGK' ların imalatında son teknoloji ürünü malzeme ve elemanlar kullanılmalıdır.</i>	
15.7.	All materials to be used in the assembly of UPSs must comply with TSE or international standards.	<i>KGK 'ların montajında kullanılacak tüm malzemeler TSE veya uluslararası standartlara uygun olmalıdır.</i>	
15.8.	Must have SNMP module.	<i>SNMP modülü olmalıdır.</i>	
15.9.	It should be able to be monitored with the Graphic Screen Remote Monitoring Panel when desired.	<i>İstenildiğinde Grafik ekranlı Uzaktan İzleme Paneli ile de izlenebilmelidir.</i>	
15.10.	Optionally, the MODBUS system must be compatible.	<i>Opsiyonel olarak MODBUS sistemi uyumlu olmalıdır.</i>	
15.11.	The Uninterruptible Power Supplies offered must be designed online and with DSP Control.	<i>Teklif edilen Kesintisiz Güç Kaynakları online olarak tasarlanmış ve DSP Kontrollü olmalıdır.</i>	
15.12.	The UPS must have a Boost charging system.	<i>KGK Boost şarj sistemine sahip olmalıdır.</i>	
15.13.	UPSs should give the output power in kVA clearly and continuously in	<i>KGK'lar, Teknik şartname de kVA cinsinden verilen çıkış gücünü net ve sürekli olarak</i>	

	the Technical specification.	<i>vermelidir.</i>	
15.14.	UPS's; It should consist of rectifier, inverter, battery charger, static and manual by-pass switch main units.	<i>KGK 'lar; Redresör, İnvertör, Akü şarjörü, Statik ve Manuel By-pass Şalteri ana ünitelerinden oluşmalıdır.</i>	
15.15.	The rectifier must have been manufactured using IPM technology. While providing the necessary DC voltage for the inverter, it should also be able to charge the batteries.	<i>Redresör IPM teknolojisi kullanılarak üretilmiş olmalıdır. İnvertör için gerekli DC gerilimi sağlarken aynı zamanda aküleri de şarj edebilmelidir.</i>	
15.16.	The inverter must be manufactured using IGBT technology and must continuously feed the load by converting the DC energy received from the rectifier or battery pack into AC energy. The inverter should operate synchronously with the grid within the limits specified in the synchronization parameters. In case of inverter failure or overload, it should transfer the load to the grid without interruption in the load supply.	<i>İnvertör, IGBT teknolojisi kullanılarak imal edilmiş olmalıdır ve redresörden yada akü grubundan aldığı DC enerjiyi AC enerjiye çevirerek, sürekli olarak yükü beslemelidir. İnvertör, senkronizasyon parametrelerinde belirtilen sınırlar içinde şebekeye senkron çalışmalıdır. İnvertör arızasında veya aşırı yük durumunda, yük beslemesinde kesinti olmaksızın yükü şebekeye aktarmalıdır.</i>	
15.17.	The battery pack must provide the necessary DC energy to the inverter in case the mains fails or the grid goes out of the specified tolerance. In case the network returns or returns within limits, the rectifier should automatically supply DC energy and the battery charger should start charging the battery group.	<i>Şebekenin kesildiği veya şebekenin belirtilen tolerans dışına çıkması durumunda akü grubu invertöre gerekli DC enerjiyi sağlamalıdır. Şebekenin geri gelmesi veya limitler içine dönmesi durumunda, redresör otomatik olarak DC enerjiyi sağlamalı, akü şarjörü akü grubunu şarj etmeye başlamalıdır.</i>	

15.18.	In order to save energy in the proposed uninterruptible power supplies, economical operating mode (Ecomode) should be optional.	<i>Teklif edilen Kesintisiz güç kaynaklarında enerji tasarrufu amacıyla opsiyonel olarak ekonomik çalışma modu (Ecomode) olmalıdır.</i>	
15.19.	In case of failure, the UPS should be able to disable itself depending on the location and nature of the failure. The faults should be visible on the panel on the UPS with the illuminated LEDs or on the LCD panel.	<i>Arıza durumunda, arızanın yerine ve mahiyetine göre KGK kendisini devre dışı bırakabilmelidir. Arızalar KGK üzerindeki panelden ışıklı LED 'lerle veya LCD panel üzerinden görülebilmelidir.</i>	
15.20.	128 historical events and 5000 alarms must be able to be kept in the memory.	<i>Geçmişe yönelik 128 adet olay ve 5000 alarmı hafızada tutulabilmelidir.</i>	
15.21.	There should also be a manual by-pass unit in order to facilitate maintenance operations.	<i>Bakım işlemlerinde kolaylık sağlaması amacıyla ayrıca manuel by-pass ünitesi de bulunmalıdır.</i>	
15.22.	In order to facilitate maintenance / repair and minimize maintenance time, UPS's microprocessor circuits and circuit boards should be in easily accessible locations and in a replaceable manner in case of malfunction.	<i>Bakım/onarımın kolaylaştırılması ve bakım süresinin asgari seviyeye indirilmesi amacıyla KGK'ların mikroişlemci devreleri ile devre kartları kolay ulaşılabilir yerlerde ve arıza durumunda değiştirilebilir şekilde olmalıdır.</i>	
15.23.	UPS must be working in parallel at least up to 4 units.	<i>KGK' en az 4 adete kadar paralel çalışıyor olmak zorundadır.</i>	
15.24.	The technical service has to present the training certificates in the offer attachment.	<i>Teknik servisin eğitim sertifikalarını teklif ekinde sunmak zorundadır.</i>	
15.25.	Input characteristics • Input Voltage and Tolerance : 220VAC (1Phase N) $\pm$ 20% • Input Frequency and Tolerance : 40-65hz	<i>Giriş karakteristikleri</i> • Giriş Gerilim ve Toleransı :220VAC (1FAZ, N) $\pm$ %20 • Giriş Frekansı ve Toleransı :40-65Hz	

	• Bypass voltage and Tolerance : the first phase 220 ± 10% • System Input Power Factor : 0.99 • Input Current THD : <5%	• <i>By-Pass Gerilimi ve Toleransı :220 1 faz ± %10</i> • <i>Sistem Giriş Güç Faktörü :0,99</i> • <i>Giriş Akım THD :<%5</i>	
15.26.	Output Characteristics • Output Power : 15 kVA • Power Kw : 10.5 kW • Output Waveform : sinusoidal • Output Voltage : 220 VAC • Output Voltage Tolerance : +/- 1% • Output Power Factor : 0.7 • Output Frequency : 50 Hz • Output Frequency Tolerance : +/- %0.2 • Efficiency at 100% load :> 92% • Crest Factor : 3: 1 • Overload : 10 minutes at 100-125% load. • Output Voltage at Linear Load : <3% • Acoustic Noise : <50 dBA	<i>Çıkış Karakteristikleri</i> • <i>Çıkış Gücü :15 kVA</i> • <i>Güç Kw :10.5 kW</i> • <i>Çıkış Dalga Şekli : Sinusoidal</i> • <i>Çıkış Gerilimi : 220 VAC</i> • <i>Çıkış Gerilim Toleransı : +/- %1</i> • <i>Çıkış Güç Faktörü : 0,7</i> • <i>Çıkış Frekansı : 50 Hz</i> • <i>Çıkış Frekans Toleransı : +/- %0.2</i> • <i>Verim %100 yükte : >%92</i> • <i>Crest Faktörü : 3:1</i> • <i>Aşırı Yük : %100-125 yükte 10 dk.</i> • <i>Çıkış Gerilimi Lineer Yükte : < %3</i> • <i>Akustik Gürültü : < 50 dba</i>	
15.27.	It must be in a structure that can keep the battery group in float charge while feeding the inverter at full load by converting the one-phase alternating voltage received from the network to the regulated correct voltage.	<i>Şebekeden aldığı bir fazlı alternatif gerilimi regüle edilmiş doğru gerilime çevirerek invertörü tam yükte beslerken akü grubunu tampon şarjda tutabilecek yapıda olmalıdır.</i>	
15.28.	The rectifier must have soft start feature. The current drawn during soft	<i>Redresör soft start özelliğine sahip olmalıdır. Soft start esnasında çekilen akım cihazın</i>	

	start should not be more than the rated current of the device. Even if the input voltage is cut for a very short time (the situation where the rectifier DC bus does not reach zero completely), it should draw current in accordance with the soft start feature.	<i>anma akımından fazla olmamalıdır. Giriş geriliminin çok kısa süreli kesilmesinde dahi (doğrultucu DC barasının tamamen sıfıra erişmediği durum) soft start özelliğine uygun akım çekmelidir.</i>	
15.29.	In case of mains power cut, input voltage and frequency out of specified tolerance values, and in cases such as phase cut, the rectifier will be automatically deactivated and the inverter will be fed through the battery . In case the appropriate voltage and frequency to be provided from the network or generator is restored, the rectifier will automatically re-engage and feed the inverter.	<i>Şebeke enerjisinin kesilmesinde, giriş gerilim ve frekansının belirtilen tolerans değerleri dışına çıkmasında ve faz kesilmesi gibi durumlarda redresör otomatik olarak devreden çıkacak, invertör akü üzerinden beslenecektir. Şebeke veya jeneratörden sağlanacak uygun gerilim ve frekansın yeniden sağlanması durumunda redresör otomatik olarak tekrar devreye girerek invertörü besleyecektir.</i>	
15.30.	In order to prevent the battery cells from being damaged by excessive charging current, there will be a current limiting circuit on the charge card.	<i>Akü hücrelerinin aşırı şarj akımı ile hasarlanmasının önlenmesi amacıyla, şarj kartında akım sınırlama devresi bulunacaktır.</i>	
15.31.	Designed using IPM technology, the inverter must transfer the DC voltage from the rectifier or battery pack to a regulated and noise-free AC voltage and transfer it to the static transfer circuit.	<i>IPM teknolojisi kullanılarak tasarlanan invertör, redresör veya akü grubundan gelen DC gerilimi regüleli ve her türlü gürültüden arındırılmış bir AC gerilime çevirerek statik transfer devresine aktarmalıdır.</i>	
15.32.	The inverter should be manufactured as microprocessor controlled so that it will be continuously on.	<i>İnvertör sürekli olarak devrede kalacak şekilde mikro işlemci kontrollü olarak imal edilmiş olmalıdır.</i>	

15.33.	Output voltage should not exceed +/- 1% and frequency +/- 0.2 % (battery operation) tolerance limits.	<i>Çıkış gerilimi +/- %1 ve frekansı +/- %0.2 (Aküden çalışma) tolerans sınırlarını aşmamalıdır.</i>	
15.34.	The dynamic tolerance of the output voltage should not exceed +/- 5%. (At 100% load impulse) This tolerance should be set to $\pm 2\%$ within 20 ms at the most.	<i>Çıkış geriliminin dinamik toleransı +/- %5 'i aşmamalıdır. (% 100 yük darbesinde) Bu tolerans en çok 20 ms'n'de $\pm 2\%$ sınırlarına çekilmelidir.</i>	
15.35.	Total harmonic amount of output voltage at full load should not exceed 3% in linear loads and 5% in computer loads (CF: 3:1).	<i>Tam yükte çıkış gerilimi toplam harmonik miktarı, lineer yüklerde % 3'ü, bilgisayar yüklerinde (CF: 3:1) %5 'ü geçmemelidir.</i>	
15.36.	The inverter output must be protected against short circuits.	<i>İnvertör çıkışı kısa devrelere karşı korunmuş olmalıdır.</i>	
15.37.	The inverter must have an overheat protection circuit.	<i>İnvertörde aşırı ısı koruma devresi bulunmalıdır.</i>	
15.38.	It must be an electronically controlled semiconductor switch consisting of semi-conductors and feed the load from the inverter in the normal operation of the UPS. In case of overload, short circuit, or a failure in the inverter, the load should be transferred to the network or auxiliary source without power cut. If the inverter also fails, it must transfer the load back to the inverter. If it is out of the specified tolerance value, it should not transfer to the network.	<i>Yarı iletkenlerden meydana gelen elektronik kontrollü yarı iletken bir şalter olmalı ve KGK 'nın normal çalışması durumunda yükü invertörden beslemelidir. Aşırı yükte, kısa devre durumunda veya invertörde bir arıza meydana geldiğinde yükü enerji kesintisi olmaksızın şebekeye yada yardımcı kaynağa aktarmalıdır. Invertör de arıza geçmiş ise yükü tekrar invertöre aktarmalıdır. Belirlenen tolerans değeri dışında ise şebekeye transfer işlemini gerçekleştirmemelidir.</i>	
15.39.	As long as the grid is within the given tolerance limits, it should be able to perform automatic synchronization and phase	<i>Şebeke verilen tolerans sınırları içinde olduğu sürece invertör çıkışı ile aralarında otomatik senkronizasyon ve faz kilitlenmesi yapabilmelidir.</i>	

	locking with the inverter output. Otherwise, the inverter should be locked to its internal oscillator.	<i>Aksi durumda invertör kendi dahili osilatörüne kilitlenmelidir.</i>	
15.40.	From the LEDs on the front panel of the UPS or the LCD screen, it should be possible to learn whether the mains and the inverter output are synchronous , synchronous out-of-limit status and overload status.	<i>UPS ön panelindeki ledler veya LCD ekrandan, şebeke ile invertör çıkışının senkron olup olmadığını, senkron limit dışı durumunu ve aşırı yük durumunu öğrenilebilmelidir.</i>	
15.41.	Static transfer circuit should be able to automatically select the network or inverter under specified conditions. In synchronous operation, the transfer between the inverter and the grid should be possible without interruption.	<i>Statik transfer devresi belirtilen şartlarda şebeke veya invertör seçimini otomatik olarak yapabilmelidir. Senkron çalışmada, invertör ile şebeke arasındaki transfer kesintisiz yapılabilirdir.</i>	
15.42.	When the UPS is requested to be disabled for maintenance, repair, or other reasons, it should transfer the load to the network or auxiliary source without interruption.	<i>Bakım, onarım veya başka sebeplerle KGK ' nın devre dışı bırakılması istenildiğinde yükü şebekeye yada yardımcı kaynağa kesintisiz aktarmalıdır.</i>	
15.43.	When this switch is ON, there should be no voltage at any point in the UPS cabinet other than the input terminals.	<i>Bu şalter ON durumunda iken KGK kabini içerisinde giriş terminallerinin dışında hiçbir noktada gerilim bulunmamalıdır.</i>	
15.44.	When 220/380 V, 50 Hz mains power is cut or when the specified tolerance band is exceeded, the UPS should continue to supply the load from the dual polarity battery group. It should feed the system to be fed for 15 minutes at full load. No interruption should be	<i>220/380 V, 50 Hz şebeke enerjisi kesildiğinde yada belirtilen tolerans bandının dışına çıkıldığında KGK çift polariteli akü grubundan yükü beslemeye devam etmelidir. Beslenecek sistemi tam yükte 15 dk süreyle beslemelidir. Akü grubundan beslemeye geçişte, çıkışta herhangi bir kesinti hissedilmemelidir.</i>	

	felt in the output from the battery group to supply.		
15.45.	Batteries; completely closed, maintenance-free, dry type, stationary (suitable for being under continuous charging) rechargeable, must have a life expectancy of at least 5 years.	<i>Aküler; tamamen kapalı, bakım gerektirmeyen (maintenance-free), kuru Tip, stasyonier (sürekli şarj altında kalmaya elverişli) şarj edilebilen, en az 5 yıl ömür beklentili olmalıdır.</i>	
15.46.	Information such as battery capacity used, battery charge voltage, and current should be monitored on the LCD panel on the device and from the software.	<i>Kullanılan akü kapasitesi , akü şarj voltajı ve akımı gibi bilgilerin cihazın üzerindeki LCD panelden ve yazılımdan izlenebilmelidir.</i>	
15.47.	Batteries necessary for the maintenance of the UPS System ' from separating switching system will be found. In this state, the UPS should continue to perform its functions without a battery.	<i>Sistemin bakımı için gerektiğinde aküleri KGK 'dan ayıran anahtarlama sistemi bulunacaktır. Bu durumda iken KGK aküsüz olarak fonksiyonlarını yerine getirmeye devam etmelidir.</i>	
15.48.	The calculation of the battery group should be made using the maximum power per cell method.	<i>Akü grubunun hesabı hücre başına düşen maksimum güç yöntemiyle yapılmalıdır.</i>	
15.49.	Battery connection parts will be insulated and not touch the body. Connections between blocks should be made of flexible material.	<i>Akü bağlantı parçaları izoleli ve gövdeye temas etmeyecek şekilde olacaktır. Bloklar arası bağlantılar esnek malzemeden yapılmalıdır.</i>	
15.50.	Rectifier, Bypass inputs, and Inverter output must be protected with a breaker or fuse in the system.	<i>Sistemde Doğrultucu, Bypass girişleri ve Evirici çıkışı şalter veya sigorta ile korunmalıdır.</i>	
15.51.	The inverter must be electronically protected against overload and short circuits.	<i>Aşırı yük ve kısa devreye karşı evirici elektronik olarak korunmalıdır.</i>	
15.52.	The system must have battery overcharge and	<i>Sistem, akü aşırı şarj vedeşarj korumasına sahip olmalıdır.</i>	

	discharge protection.		
15.53.	The system must have over-heat protection.	<i>Sistem aşırı ısı korumasına sahip olmalıdır.</i>	
15.54.	The user should be able to access information about the operation of the system through the control panel of the UPS or the LCD screen. In addition, there should be a sound warning that can be silenced in case of failure or power failure.	<i>KGK' nın kontrol paneli veya LCD ekran üzerinden, kullanıcı sistemin çalışması ile ilgili bilgilere ulaşabilmelidir. Ayrıca arıza veya elektrik kesintisi durumunda susturulabilir ses ikazı olmalıdır.</i>	
15.55.	A connection with a computer must be possible with a standard RS 232 output. All information about the UPS should be displayed on the screen.	<i>Standart RS 232 çıkışı ile bilgisayar'la bağlantı kurulabilmelidir. KGK ile ilgili tüm bilgiler ekrandan izlenebilmelidir.</i>	
15.56.	As standard, the UPS should automatically shut down Novell, Windows, NT type operating systems when the electricity is cut off. The software to be provided for these operating systems must be graphic-based and given free of charge.	<i>Standart olarak UPS elektrikler kesildiğinde Novell, Windows, NT, tipi işletim sistemlerini otomatik kapatabilmelidir. Bu işletim sistemleri için verilecek yazılım grafik tabanlı olmalı ve ücretsiz olarak verilmelidir</i>	
15.57.	The UPS must be compatible to be used with SNMP and communication must be made with SNMP when required.	<i>KGK SNMP ile kullanılmaya uyumlu olmalı ve istenildiğinde haberleşme SNMP ile yapılabilmelidir.</i>	
15.58.	The UPS system must have a firmware structure so that the system must be fully software controlled. Future developments should be able to be transferred to the system with the software development function and the system should be updated.	<i>KGK sistemi firmware yapısına sahip olmalı böylece sistem tamamı ile yazılım kontrollü olmalıdır. İleride olabilecek gelişmeler yazılım geliştirme fonksiyonu ile ile sisteme aktarılabilmesi ve sistem update edilebilmelidir.</i>	

15.59.	It should have automatic and manual battery test feature.	<i>Otomatik ve manuel akü test özelliği olmalıdır.</i>	
15.60.	The Uninterruptible Power Supply must be able to operate continuously between 0 °C and 40 °C, The working altitude must be up to 1000 m and at higher levels the system must operate with excessive air circulation .	<i>Kesintisiz GüçKaynağı 0°C ile 40°C arasında sürekli çalışabilmeli, Çalışma yüksekliği 1000 m'ye kadar olmalı ve daha yukarı seviyelerde sistem, fazla hava sirkülasyonu sağlamakla çalışmalıdır.</i>	
15.61.	The amount of heat the system emits into the environment should be specified.	<i>Sistemin ortama yaymakta olduğu ısı miktarı belirtilmelidir.</i>	
15.62.	The Uninterruptible Power Supply should have a front panel in liquid crystal display (LCD) structure.	<i>Kesintisiz Güç Kaynağında likit kristal display (LCD) yapısında bir ön panel bulunmalıdır.</i>	
15.63.	The user should be able to get information about the progress of the system at a glance from this panel. Control keys and other controller keys required for the system should also be located here.	<i>Kullanıcı bu panodan sistemin gidişatı hakkında bir bakışta bilgi sahibi olabilmelidir. Sistem için gerekli olan kontrol tuşları ile diğer kontrol edici anahtarlar da burada yer almalıdır.</i>	
15.64.	The following status and alarm messages must be visible on the front panel: • Load is on Uninterruptible Power Supply • Freight By-Pass also • Manual By-Pass •Emergency shutdown • The battery voltage is low • Fault codes • Audible alarm on • Mains cut • Overload • Excessive heat • Battery low • High Battery	<i>Ön panelde aşağıdaki durum ve alarm mesajları mutlaka görülebilmelidir:</i> • Yük Kesintisiz Güç Kaynağında • Yük By-Pass da • Manuel By-Pass • Acil kapatma • Akü gerilimi düşük • Arıza kodları • Sesli alarm açık • Şebeke kesik • Aşırı yük • Aşırı ısı • Akü düşük • Akü yüksek • Çıkış düşük	

	• Output low • Output high	• Çıkış yüksek	
15.65.	In addition, the values below should be monitored on the LCD panel from the measurement menu: • Load value in% • Output voltage and frequency • Input voltage, current, and frequency • By-pass voltage and frequency • Input current • Battery voltage, battery discharge current • Battery capacity and remaining battery time • Temperature	Ayrıca aşağıda bulunan değerler ölçüm menüsünden LCD panelde izlenebilmelidir. • % olarak yük değeri • Çıkış voltajı ve frekansı • Giriş voltajı, akımı ve frekansı • By-pass voltajı ve frekansı • Giriş akımı • Akü voltajı , şarj deşarj akımı • Akü kapasitesi ve kalan akü süresi • Sıcaklık	

Product catalogue/brochure of the proposed brand/model showing detailed technical specifications of the goods should be submitted.

Other Related services and requirements (based on the information provided in Section 5b)	Compliance with requirements		Details or comments on the related requirements
	Yes, we comply	No, we cannot comply (indicate discrepancies)	
Delivery, installation and commissioning of each item within 90 calendar days following the signature of the contract			
Warranty (min. 3 years) for each item			
Local Service Support			
Training following installation			

FORM F: Price Schedule Form

Name of Bidder:	[Insert Name of Bidder]	Date:	Select date
ITB reference:	[Insert ITB Reference Number]		

The Bidder is required to prepare the Price Schedule following the below format.

The price shall not include value added tax (VAT) since UN and its subsidiary organs are exempt from all taxes except the special consumption tax.

Currency of the Bid: United States Dollars (USD)

Price Schedule

Item / Ürün #	Description of Goods // Malın Tanımı	UOM // Ölçüm Birimi	Quantity // Miktar	Unit Price // Birim Fiyat (USD)	Total Price // Toplam Fiyat (USD)
1	Server // Sunucu	Pieces // Adet	2		
2	Data Storage Unit // Veri Depolama Ünitesi	Pieces // Adet	1		
3	Virtualization Software // Sanallaştırma Yazılımı	Pieces // Adet	1		
4	Backup Software // Yedekleme Yazılımı	Pieces // Adet	1		
5	Server Software // Sunucu Yazılımları (80 core Windows Server 2019 Standard licenses or equivalent 20 Windows Server 2019 Cal licenses or equivalent 2 SQL Server 2019 licenses or equivalent 20 SQL Server 2019 Cal licenses or equivalent)	Lump Sum // Götürü Bedel	1		
6	Backup Unit // Yedekleme Ünitesi	Pieces // Adet	1		

7	Network Switch Type 1 // Ağ anahtarı Tip 1	Pieces // Adet	1		
8	Network Switch Type 2 (non-POE) // Ağ anahtarı Tip 2 (POE Olmayan)	Pieces // Adet	2		
9	Wireless Access Point // Kablosuz Erişim Noktası	Pieces // Adet	7		
10	Authentication and Network Access Control Software // Kimlik Doğrulama ve Ağ Erişim Kontrol Yazılımı	Pieces // Adet	1		
11	Firewall // Güvenlik Duvarı	Pieces // Adet	1		
12	Personal Computer // Bilgisayar	Pieces // Adet	2		
13	Data Center Security Software // Veri Merkezi Güvenlik Yazılımı	Pieces // Adet	1		
14	User Security Solution // Kullanıcı Güvenliği Çözümü	Pieces // Adet	1		
15	Uninterruptable Power Supply // Kesintisiz Güç Kaynağı	Pieces // Adet	2		
Total Final and All-Inclusive Turnkey Bid Price* (USD) <i>Anahtar Teslim Toplam kesin ve her şey dahil fiyat teklifi</i>					

*The Contractor shall not be entitled to receive any price difference and/or additional amount from UNDP for whatsoever reason, including but not limited to increase in the costs of the Contractor or any missing goods/services in its Price Schedule to be submitted in response to this ITB.

*100% of the payment will be made within 30 days upon UNDP's issuance of Positive Inspection and Acceptance Report that indicates full compliance of the goods to Technical Specifications in this ITB and proper functioning of the whole system and receipt of invoice.

Name of Bidder: _____

Authorised signature: _____

Name of authorised signatory: _____

Functional Title: _____

FORM G: Form of Bid Security

**Bid Security must be issued using the official letterhead of the Issuing Bank.
Except for indicated fields, no changes may be made on this template.**

To: UNDP
[Insert contact information as provided in Data Sheet]

WHEREAS [Name and address of Bidder] (hereinafter called "the Bidder") has submitted a Bid to UNDP dated [Click here to enter a date](#) to execute goods and/or services [Insert Title of Goods and/or Services] (hereinafter called "the Bid"):

AND WHEREAS it has been stipulated by you that the Bidder shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security if the Bidder:

- a) Fails to sign the Contract after UNDP has awarded it;
- b) Withdraws its Bid after the date of the opening of the Bids;
- c) Fails to comply with UNDP's variation of requirement, as per ITB instructions; or
- d) Fails to furnish Performance Security, insurances, or other documents that UNDP may require as a condition to rendering the contract effective.

AND WHEREAS we have agreed to give the Bidder such Bank Guarantee:

NOW THEREFORE we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Bidder, up to a total of *[amount of guarantee] [in words and numbers]*, such sum being payable in the types and proportions of currencies in which the Price Bid is payable, and we undertake to pay you, upon your first written demand and without cavil or argument, any sum or sums within the limits of *[amount of guarantee as aforesaid]* without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

This guarantee shall be valid up to 30 days after the final date of validity of bid.

SIGNATURE AND SEAL OF THE GUARANTOR BANK

Signature: _____

Name: _____

Title: _____

Date: _____

Name of Bank _____

Address _____

[Stamp with official stamp of the Bank]

[insert: address and email address]