



PHILIPPINE BIDDING DOCUMENTS

(As Harmonized with Development Partners)

Procurement of 720 Licenses and Support Maintenance for Endpoint Security

Bid Reference No.: ITB-ITD-007-25-04-2023

Government of the Republic of the Philippines

*Approved Budget for the Contract is
One Million Nine Hundred Twenty Thousand Pesos
Only (Php 1,920,000.00)*

*Covered Period: One (1) Year
Effective Date: August 27, 2023*

Sixth Edition
July 2020

A handwritten signature in black ink, appearing to read "D. A.", located at the bottom right corner of the page.

Table of Contents

| | |
|--|----|
| Glossary of Acronyms, Terms, and Abbreviations | 2 |
| Section I. Invitation to Bid..... | 5 |
| Section II. Instructions to Bidders..... | 8 |
| 1. Scope of Bid | 9 |
| 2. Funding Information..... | 9 |
| 3. Bidding Requirements | 9 |
| 4. Corrupt, Fraudulent, Collusive, and Coercive Practices | 9 |
| 5. Eligible Bidders..... | 10 |
| 6. Origin of Goods | 10 |
| 7. Subcontracts | 10 |
| 8. Pre-Bid Conference | 10 |
| 9. Clarification and Amendment of Bidding Documents | 10 |
| 10. Documents comprising the Bid: Eligibility and Technical Components | 10 |
| 11. Documents comprising the Bid: Financial Component | 11 |
| 12. Bid Prices | 11 |
| 13. Bid and Payment Currencies | 12 |
| 14. Bid Security | 12 |
| 15. Sealing and Marking of Bids | 12 |
| 16. Deadline for Submission of Bids | 13 |
| 17. Opening and Preliminary Examination of Bids | 13 |
| 18. Domestic Preference | 13 |
| 19. Detailed Evaluation and Comparison of Bids | 13 |
| 20. Post-Qualification | 14 |
| 21. Signing of the Contract | 17 |
| Section III. Bid Data Sheet | 18 |
| Section IV. General Conditions of Contract | 20 |
| 1. Scope of Contract | 21 |
| 2. Advance Payment and Terms of Payment | 21 |
| 3. Performance Security | 21 |
| 4. Inspection and Tests | 21 |
| 5. Warranty | 22 |
| 6. Liability of the Supplier | 22 |
| Section V. Special Conditions of Contract | 23 |
| Section VI. Schedule of Requirements | 26 |
| Section VII. Technical Specifications | 27 |
| Section VIII. Checklist of Technical and Financial Documents | 67 |



Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

Bid – A signed offer or proposal to undertake a contract submitted by a bidder in response to and in consonance with the requirements of the bidding documents. Also referred to as *Proposal* and *Tender*. (2016 revised IRR, Section 5[c])

Bidder – Refers to a contractor, manufacturer, supplier, distributor and/or consultant who submits a bid in response to the requirements of the Bidding Documents. (2016 revised IRR, Section 5[d])

Bidding Documents – The documents issued by the Procuring Entity as the bases for bids, furnishing all information necessary for a prospective bidder to prepare a bid for the Goods, Infrastructure Projects, and/or Consulting Services required by the Procuring Entity. (2016 revised IRR, Section 5[e])

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

Consulting Services – Refer to services for Infrastructure Projects and other types of projects or activities of the GOP requiring adequate external technical and professional expertise that are beyond the capability and/or capacity of the GOP to undertake such as, but not limited to: (i) advisory and review services; (ii) pre-investment or feasibility studies; (iii) design; (iv) construction supervision; (v) management and related services; and (vi) other technical services or special studies. (2016 revised IRR, Section 5[i])

CDA - Cooperative Development Authority.

Contract – Refers to the agreement entered into between the Procuring Entity and the Supplier or Manufacturer or Distributor or Service Provider for procurement of Goods and Services; Contractor for Procurement of Infrastructure Projects; or Consultant or Consulting Firm for Procurement of Consulting Services; as the case may be, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.



CPI – Consumer Price Index.

DDP – Refers to the quoted price of the Goods, which means “delivered duty paid.”

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – “Free Carrier” shipping point.

FOB – “Free on Board” shipping point.

Foreign-funded Procurement or Foreign-Assisted Project– Refers to procurement whose funding source is from a foreign government, foreign or international financing institution as specified in the Treaty or International or Executive Agreement. (2016 revised IRR, Section 5[b]).

Framework Agreement – Refers to a written agreement between a procuring entity and a supplier or service provider that identifies the terms and conditions, under which specific purchases, otherwise known as “Call-Offs,” are made for the duration of the agreement. It is in the nature of an option contract between the procuring entity and the bidder(s) granting the procuring entity the option to either place an order for any of the goods or services identified in the Framework Agreement List or not buy at all, within a minimum period of one (1) year to a maximum period of three (3) years. (GPPB Resolution No. 27-2019)

GFI – Government Financial Institution.

GOCC – Government-owned and/or –controlled corporation.

Goods – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term “related” or “analogous services” shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.



Infrastructure Projects – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

Procurement Project – refers to a specific or identified procurement covering goods, infrastructure project or consulting services. A Procurement Project shall be described, detailed, and scheduled in the Project Procurement Management Plan prepared by the agency which shall be consolidated in the procuring entity's Annual Procurement Plan. (GPPB Circular No. 06-2019 dated 17 July 2019)

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

Supplier – refers to a citizen, or any corporate body or commercial company duly organized and registered under the laws where it is established, habitually established in business and engaged in the manufacture or sale of the merchandise or performance of the general services covered by his bid. (Item 3.8 of GPPB Resolution No. 13-2019, dated 23 May 2019). Supplier as used in these Bidding Documents may likewise refer to a distributor, manufacturer, contractor, or consultant.

UN – United Nations.

Section I. Invitation to Bid



INVITATION TO BID FOR

Procurement of 720 Licenses and Support Maintenance for Endpoint Security

1. The **UCPB Savings, Inc. (UCPBS)**, through the *Approved Corporate Budget (ABC) of Year 2023*, intends to apply the sum of *One Million Nine Hundred Twenty Thousand Pesos Only (Php1,920,000.00), inclusive of all applicable taxes and other charges, including insurance coverage (if applicable)* for the Procurement of **720 Licenses and Support Maintenance for Endpoint Security** – Project Identification Number: **ITB-ITD-007-25-04-2023**, being the ABC to payments under the contract. Bids received in excess of the ABC shall be automatically rejected at bid opening.
2. The **UCPBS** now invites bids for the above Procurement Project. Delivery of the Goods shall *take effect on August 27, 2023 and shall cover a period of one (1) full calendar year*. Bidders should have completed, within 2 years prior to the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).
3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary “*pass/fail*” criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.
 - a. Bidding is open to all interested bidders, whether local or foreign, subject to the conditions for eligibility provided in the 2016 revised IRR of RA No. 9184.
4. Prospective Bidders may obtain further information from **UCPB Savings, Inc. (UCPBS)** and inspect the Bidding Documents at the address given below during office hours from 8:30am to 3:00pm.
5. A complete set of Bidding Documents may be acquired by interested Bidders on **May 12, 2023 to May 22, 2023** from the given address and website(s) below *and upon payment of the applicable fee for the Bidding Documents, pursuant to the latest Guidelines issued by the GPPB, in the amount of Php5,000.00*.

Instructions to bidders on payment of bid documents:

- a. The payment for the Bid Documents shall be limited to Cash or Manager's/ Cashier's Check payable to UCPB Savings. Personal checks shall not be accepted.
- b. The Bidder is required to enclose the cover page of this Invitation to Bid (ITB) in order to properly determine which bid document, the bidder is paying for.



- c. It may also be downloaded from the website of the Philippine Government Electronic Procurement System (PhilGEPS) and the website of the Procuring Entity, provided that the Bidders shall pay the applicable fee for the Bidding Documents not later than the submission of their bids.
- 6. The **UCPB Savings (UCPBS)** will hold a Pre-Bid Conference¹ on **May 23, 2023/ Tuesday at 2:30pm** via MS Teams, which shall be open to prospective bidders. Interested bidders are requested to coordinate with the BAC Secretariat for the MS Teams link.
- 7. Bids must be duly received by the BAC Secretariat through (i) manual submission at the office address indicated on or before **11:30am of May 30, 2023/ Tuesday**. Late bids shall not be accepted.
- 8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **IB Clause 14**.
- 9. Bid opening shall be on **May 30, 2023/ Tuesday at 2:30pm** via MS Teams. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.
- 10. The **UCPB Savings (UCPBS)** reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.
- 11. For further information, please refer to:

DRONNEL A. ESPINA

BAC Secretariat

UCPB SAVINGS, INC.

2nd Floor, Overseas Filipino (OF) Bank Center Building, 1000 Liwasang Bonifacio
Intramuros, Barangay 656-A, 1000 Manila City, Philippines

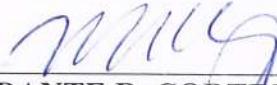
Trunkline number: (+632)

Email Address: bacsecretariat@ucpbsavings.com

- 12. You may visit the following websites:

For downloading of Bidding Documents: <https://www.ucpbsavings.com>

[Date of Issue]


DANTE R. CORTEZ
BAC Chairperson

¹ May be deleted in case the ABC is less than One Million Pesos (PhP1,000,000) where the Procuring Entity may not hold a Pre-Bid Conference.

Section II. Instructions to Bidders



1. Scope of Bid

The Procuring Entity, ***UCPB Savings (UCPBS)*** wishes to receive Bids for the ***Procurement of 720 Licenses and Support Maintenance for Endpoint Security***, with identification number **ITB-ITD-007-25-04-2023**

The delivery of the Goods shall take effect on August 27, 2023 and shall cover a period of one (1) full calendar year. The Procurement Project (referred to herein as “Project”) covers 1 item, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

- 2.1. The GOP through the source of funding as indicated below for ***Year 2023*** in the amount of ***One Million Nine Hundred Thousand Pesos Only (Php1,920,000.00), inclusive of all applicable taxes and other charges, including insurance coverage if applicable.***
- 2.2. The source of funding is the corporate budget of UCPBS or procuring entity

3. Bidding Requirements

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex “I” of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.



5. Eligible Bidders

- 5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.
- 5.2. Foreign ownership exceeding those allowed under the rules may participate in this Project.
- 5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to:
 - a. For the procurement of Non-expendable Supplies and Services: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.
- 5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

6. Origin of Goods

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **IB** Clause 18.

7. Subcontracts

- 7.1. The Procuring Entity has prescribed that subcontracting is not allowed.

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time indicated in paragraph 6 of the **ITB**.

9. Clarification and Amendment of Bidding Documents

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

- 10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.
- 10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within **3 years** prior to the deadline for the submission and receipt of bids.
- 10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

11. Documents comprising the Bid: Financial Component

- 11.1. The second bid envelope shall contain the financial documents for the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.
- 11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.
- 11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **ITB** shall not be accepted.
- 11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

12. Bid Prices

- 12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:
 - a. For Goods offered from within the Procuring Entity's country:
 - i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);
 - ii. The cost of all customs duties and sales and other taxes already paid or payable;

- iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and
 - iv. The price of other (incidental) services, if any, listed in e.
- b. For Goods offered from abroad:
- i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.
 - ii. The price of other (incidental) services, if any, as listed in **Section VII (Technical Specifications)**.

13. Bid and Payment Currencies

- 13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.
- 13.2. Payment of the contract price shall be made in:
 - a. Philippine Pesos.

14. Bid Security

- 14.1. The Bidder shall submit a Bid Securing Declaration² or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.
- 14.2. The Bid and bid security shall be valid for **120 days** from the date of bid opening. Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

Each Bidder shall submit one copy of the first and second components of its Bid.

² In the case of Framework Agreement, the undertaking shall refer to entering into contract with the Procuring Entity and furnishing of the performance security or the performance securing declaration within ten (10) calendar days from receipt of Notice to Execute Framework Agreement.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.

16. Deadline for Submission of Bids

- 16.1. The Bidders shall submit on the specified date and time and either at its physical address as indicated in paragraph 7 of the **ITB**.

17. Opening and Preliminary Examination of Bids

- 17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **ITB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

- 17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

18. Domestic Preference

- 18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

19. Detailed Evaluation and Comparison of Bids

- 19.1. The Procuring BAC shall immediately conduct a detailed evaluation of all Bids rated “*passed*,” using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.
- 19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **IB** Clause 15 shall be submitted for each lot or item separately.

- 19.3. The descriptions of the lots or items shall be indicated in **Section VII (Technical Specifications)**, although the ABCs of these lots or items are indicated in the **BDS** for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the 2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.
- 19.4. The Project shall be awarded as **one contract**.
- 19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

20. Post-Qualification

- 20.1. The Lowest Calculated Bid/Highest Rated Bid shall undergo post-qualification in order to determine whether the bidder concerned complies with and is responsive to all the requirements and conditions as specified in the Bidding Documents.
- 20.2. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

Failure to submit any of the post-qualification requirements on time, or a finding against the veracity thereof, shall disqualify the bidder for award: Provided, That in the event that a finding against the veracity of any of the documents submitted is made, it shall cause the forfeiture of the Bid Security in accordance with Section 69 of this IRR.(a)

- 20.3. The post-qualification shall verify, validate, and ascertain all statements made and documents submitted by the bidder with the Lowest Calculated Bid/Highest Rated Bid, using non-discretionary criteria, as stated in the Bidding Documents. These criteria shall consider, but shall not be limited to, the following:
 - a) Legal Requirements. To verify, validate, and ascertain licenses, certificates, permits, and agreements submitted by the bidder, and the fact that it is not included in any “blacklist” as provided in Section 25.3 of this IRR. For this purpose, the GPPB shall maintain a consolidated file of all “blacklisted” suppliers, contractors, and consultants.

b) Technical Requirements. To determine compliance of the goods, infrastructure projects, or consulting services offered with the requirements specified in the Bidding Documents, including, where applicable:

- i) Verification and validation of the bidder's stated competence and experience, and the competence and experience of the bidder's key personnel to be assigned to the project, for the procurement of Infrastructure Projects and Consulting Services;
- ii) Verification of availability and commitment, and/or inspection and testing for the required capacities and operating conditions, of equipment units to be owned/leased/under purchase by the bidder for use in the contract under bidding, as well as checking the performance of the bidder in its ongoing government and private contracts, if any of these ongoing contracts shows:
 - a. Negative slippage of at least fifteen percent (15%) in any one project or a negative slippage of at least ten percent (10%) in each of two (2) or more contracts;
 - b. Failure of the contractor to commence repair works on ongoing contracts within seven (7) calendar days and to complete them within thirty (30) calendar days after receipt of the Procuring Entity's notice of defects and deficiencies;
 - c. Failure of the contractor to commence repair works on contracts with pending certificates of acceptance within thirty (30) calendar days and complete them within ninety (90) days after receipt of the Procuring Entity's notice of defects and failures; or
 - d. Substandard quality of work as per contract plans and specifications, or unsatisfactory performance of the contractor's obligations as per contract terms and conditions, at the time of inspection.

If the BAC verifies any of these deficiencies to be due to the contractor's fault or negligence, the agency shall disqualify the contractor from the award, for the procurement of Infrastructure Projects.

iii) Verification and/or inspection and testing of the goods/product, after-sales and/or maintenance capabilities, in applicable cases, as well as checking the following:

- a. Delay in the partial delivery of goods amounting to ten percent (10%) of the contract price in its ongoing government and private contracts;
- b. If any of these contracts shows the bidder's failure to deliver or perform any or all of the goods or services within the period(s) specified

in the contract or within any extension thereof granted by the Procuring Entity pursuant to a request made by the supplier prior to the delay, and such failure amounts to at least ten percent (10%) of the contract price; or

c. Unsatisfactory performance of the supplier's obligations as per contract terms and conditions at the time of inspection.

If the BAC verifies any of these deficiencies to be due to the bidder's fault or negligence, the BAC shall disqualify the bidder from the award, for the procurement of Goods.

iv) Ascertainment of the authenticity of the bid security and its correctness as to type, amount, form and wording, and validity period, as required in the Bidding Documents.

c) Financial Requirements. To verify, validate and ascertain the bid price proposal of the bidder and, whenever applicable, the required committed Line of Credit in the amount specified and over the period stipulated in the Bidding Documents, or the bidder's NFCC to ensure that the bidder can sustain the operating cash flow of the transaction.

- 20.4 If the BAC determines that the bidder with the Lowest Calculated Bid/Highest Rated Bid passes all the criteria for post-qualification, it shall declare the said bid as the LCRB or HRRB, and recommend to the HoPE the award of contract to the said bidder at its submitted bid price or its calculated bid price, whichever is lower or, in the case of quality-based evaluation procedure, submitted bid price or its negotiated price, whichever is lower.
- 20.5 If, however, the BAC determines that the bidder with the Lowest Calculated Bid/Highest Rated Bid fails the criteria for post-qualification, it shall immediately notify the said bidder in writing of its post-disqualification and the grounds for it.
- 20.6 Immediately after the BAC has notified the first bidder of its post-disqualification, and notwithstanding any pending request for reconsideration thereof, the BAC shall initiate and complete the same post-qualification process on the bidder with the second Lowest Calculated Bid/Highest Rated Bid. If the second bidder passes the post-qualification, and provided that the request for reconsideration of the first bidder has been denied, the second bidder shall be post-qualified as the bidder with the LCRB or HRRB.
- 20.7 If the second bidder, however, fails the post-qualification, the procedure for post-qualification shall be repeated for the bidder with the next Lowest Calculated Bid/Highest Rated Bid, and so on until the LCRB or HRRB, as the case may be, is determined for award, subject to Section 37 of this IRR.

- 20.8 The post-qualification process shall be completed in not more than twelve (12) calendar days from the determination of the Lowest Calculated Bid/Highest Rated Bid. In exceptional cases, the post-qualification period may be extended by the HoPE, but in no case shall the aggregate period exceed forty-five (45) calendar days for Goods and Infrastructure Projects, or thirty (30) calendar days in Consulting Services.

In case of post-disqualification of the bidder with the lowest calculated bid/highest rated bid, the BAC shall be given the same fresh period to conduct the post-qualification of the next lowest calculated bid/highest rated bid until a bidder is post-qualified or failure of bidding is declared based on Section 35.1(c) of this IRR.

21. Signing of the Contract

- 21.1. The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS**.

Section III. Bid Data Sheet



Bid Data Sheet

| ITB/ IB Clause | |
|----------------|--|
| 5.3 | For this purpose, contracts similar to the Project shall be: a. <i>Procurement of 720 Licenses and Support Maintenance for Endpoint Security</i> |
| 7.1 | <i>Subcontracting is not allowed.</i> |
| 12 | The price of the Goods shall be quoted DDP <i>UCPB Savings at 2nd Floor, Overseas Filipino Bank Center Building, 1000 Liwasang Bonifacio, Intramuros, Barangay 656-A, 1000 Manila City.</i> |
| 14.1 | The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts: a. The amount of not less than Php38,400.00 (2% of ABC) , if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; or b. The amount of not less than Php96,000.00 (5% of ABC) , if bid security is in Surety Bond. |
| 19.3 | <i>One Lot –Procurement of 720 Licenses and Support Maintenance for Endpoint Security</i> |
| 20.2 | In case the bidder opted to submit their Class "A" Documents as part of the eligibility documents during bid submission, the Certificate of PhilGEPS Registration (Platinum Membership) shall remain as a post-qualification requirement to be submitted in accordance with Section 34.2 of the 2016 Revised IRR of RA 9184. |
| 21.2 | <i>Non-Disclosure Agreement (NDA) –form to be provided by end-user</i> |



Section IV. General Conditions of Contract



1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract (SCC)**.

2. Advance Payment and Terms of Payment

- 2.1. Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.
- 2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the **SCC**.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC, Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.



All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

- 6.1. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.
- 6.2. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section V. Special Conditions of Contract

A handwritten signature in black ink, appearing to read "John Doe".

Special Conditions of Contract

| GCC Clause | |
|------------|---|
| 1 | <p><i>Additional requirements for the completion of this Contract:</i></p> <ol style="list-style-type: none"> 1. License Certificate / Certificate of Entitlement |
| | <p>Delivery and Documents –</p> <p>For purposes of the Contract, “EXW,” “FOB,” “FCA,” “CIF,” “CIP,” “DDP” and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows:</p> <p><i>[For Goods supplied from abroad, state:]</i> “The delivery terms applicable to the Contract are DDP delivered to UCPBS Head Office. In accordance with INCOTERMS.”</p> <p><i>[For Goods supplied from within the Philippines, state:]</i> “The delivery terms applicable to this Contract are delivered <i>UCPBS Head Office</i>. Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination.”</p> <p>Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements).</p> <p>For purposes of this Clause the Procuring Entity’s Representative at the Project Site is:</p> <p style="text-align: center;">DRONNEL A. ESPINA <i>BAC Secretariat</i> UCPB SAVINGS, INC. <i>2nd Floor, Overseas Filipino (OF) Bank Center Building,</i> <i>1000 Liwasang Bonifacio, Intramuros, Barangay 656-A</i> <i>1000 Manila City, Philippines</i> <i>Trunkline no. (+632) 8555-1018 local 1005</i> <i>Email Address: bacsecretariat@ucpbsavings.com</i></p> |
| | <p>Incidental Services –</p> <p>The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements:</p> |



| GCC Clause | | | | | | | | | | |
|------------|--|------------------------|-----------------------------------|------------------------|---|---|-----|---|---------------------|-----|
| | <p>The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.</p> <p>Spare Parts – Not applicable</p> <p>Packaging – Not applicable</p> <p>Insurance – Not applicable</p> <p>Transportation – Not applicable</p> | | | | | | | | | |
| | <p>Intellectual Property Rights –</p> <p>The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.</p> | | | | | | | | | |
| 2.2 | <p>The terms of payment shall be as follows:</p> <table border="1"> <thead> <tr> <th>Payment</th> <th>Deliverables/ Detailed Activities</th> <th>Percentage of Payments</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Certificate of Entitlement / Proof of Support</td> <td>50%</td> </tr> <tr> <td>2</td> <td>License Certificate</td> <td>50%</td> </tr> </tbody> </table> | Payment | Deliverables/ Detailed Activities | Percentage of Payments | 1 | Certificate of Entitlement / Proof of Support | 50% | 2 | License Certificate | 50% |
| Payment | Deliverables/ Detailed Activities | Percentage of Payments | | | | | | | | |
| 1 | Certificate of Entitlement / Proof of Support | 50% | | | | | | | | |
| 2 | License Certificate | 50% | | | | | | | | |

Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

| Item Number | Description | Quantity | Total | Delivered, Weeks/Months |
|--------------------|---|-----------------|--------------|--|
| 1 | Certificate of Entitlement / Proof of Support | 1 | 1 | Within 1 week from the effective date of the contract and upon issuance of NTP. |
| 2 | License Certificate | 720 | 720 | Within 1 month from the effective date of the contract and upon issuance of NTP. |

Section VII. Technical Specifications

A handwritten signature in black ink, appearing to read "John Doe". It is positioned at the bottom right corner of the page.

Technical Specifications

*Procurement of 720 Licenses and Support Maintenance for Endpoint Security
(ITB-ITD-007-25-04-2023)*

| Item # | TECHNICAL SPECIFICATIONS | |
|---------------|---|--|
| | General Requirements | |
| 1 | <p>The IT services to be rendered by Supplier to UCPBS shall be technical support and maintenance services defined as:</p> <ol style="list-style-type: none"> 1 Any task or activity done by Supplier through electronic mail, telephone, messaging platforms (e.g., Viber, WhatsApp) or on-site presence, for the purpose of providing technical support, hardware and software maintenance, or assistance to UCPBS to troubleshoot, configure, update and check the performance of the Solution 2 Technical Support and/or assistance shall include; the provision of analysis and recommendations and the performance or fulfillment of the recommendation/s. 3 Technical Support Services shall be available from Mondays through Sundays, 24x7 (working-hours and non-working hours). | |
| 4 | <p><u>Location/s of Covered Components:</u></p> <ol style="list-style-type: none"> 1. 2nd floor, Overseas Filipino (OF) Bank Center Building, 1000 Liwasang Bonifacio, Intramuros, Barangay 656-A, 1000 Manila City, Philippines; 2. 2nd floor, UCPBS Disaster Recovery Site, 721 Aurora Blvd., Quezon City, Philippines | |
| 5 | <p><u>Scope of Local Support Services</u></p> <ol style="list-style-type: none"> a. The Supplier, through a Service or Help Desk, shall provide technical support assistance by electronic mail, telephone, and messaging platforms. b. The Supplier's Service Desk shall be staffed with technically competent support engineers. The Service Desk shall be the single point-of-contact for UCPBS for Local Support Services. c. Service Desk operations shall be supported by the Supplier's internal electronic ticketing system, along with the necessary electronic mail and telephony systems. d. For support requests that cannot be resolved remotely, On-site support shall be provided by Supplier | <p><u>Statement of Compliance</u></p> |
| 6 | <p><u>Support Level</u></p> <p>Supplier shall directly provide Levels 1 and 2 Technical Support to UCPBS's support requests. These Levels are defined as:</p> <ul style="list-style-type: none"> • Level 1 Technical Support – First-line support involving the tasks of problem identification, understanding UCPBS's | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <p>expectations, initial problem diagnosis, and basic technical troubleshooting based on Supplier's knowledgebase of known problems and resolutions.</p> <ul style="list-style-type: none"> • Level 2 Technical Support – Advanced Support involving the tasks of complex problem identification, in-depth problem diagnosis, and advanced technical troubleshooting. In some cases, if necessary, reproduction of the problem by Supplier, in coordination with UCPBS, is necessary to arrive at a solution. <p>Supplier shall facilitate resolution of support requests requiring Levels 3 and 4 support involving 3rd party supplier(s), including the Manufacturers-Principals, who developed and who have intellectual property rights over the Solution. These levels are defined as:</p> <ul style="list-style-type: none"> • Level 3 Technical Support – Support of this nature will require the involvement of the 3rd party supplier to conduct research and development to a new and/or unknown issue. Such issues shall require solutions such as bug fix, error correction, custom engineering or interim patch or fix for the Solution to operate as required by UCPBS, which only the 3rd Party supplier may provide. • Level 4 Technical Support – Support of this nature will involve the 3rd Party supplier's integration of the resolution to the Solution as an official patch, feature or capability. <p>Regardless of Support Level, UCPBS's concerns, incidents and queries may be referred to the 3rd Party supplier from whom the supported Solution originated without any additional cost to UCPBS.</p> |
| 7 | <p><u>Service Management and Reporting</u></p> <ul style="list-style-type: none"> • Supplier shall handle and manage UCPBS's service requests in accordance with workflow procedures approved by UCPBS. • Quarterly reports on support requests and reported incidents will be completed by Supplier and submitted to UCPBS. • Quarterly status reports will be discussed by the Supplier Account Service Manager with UCPBS to ensure that UCPBS is aware of possible support issues and risks faced by UCPBS. |



| Item # | TECHNICAL SPECIFICATIONS | | |
|--------|---|--------------------|------------------------|
| 8 | Service Level Agreement | | |
| | Severity Level | Max. Response Time | Max. Time Until Onsite |
| | 1 | 2 Hours | 4 Hours |
| | 2 | 3 Hours | 8 Hours |
| | 3 | 4 Hours | 2 Days |
| | 4 | 6 Hours | 4 Days |
| | 5 | 1 Day | N.A. |
| | Severity Level 1 | | |
| | <ul style="list-style-type: none"> • Failure which causes major impact to UCPBS Business • Covered Solution or System is not operational. | | |
| | Examples: | | |
| | <ul style="list-style-type: none"> • System Hang (unable to save work in progress) • System functionality failure causes data losses or system unusable; • System down • Functionality failure renders system ineffective | | |
| | Severity Level 2 | | |
| | <ul style="list-style-type: none"> • Failure causing severe degradation of UCPBS business • Covered Solution or System is not operating with full capability but is still operational. | | |
| | Examples: | | |
| | <ul style="list-style-type: none"> • Impaired or broken functionality with significant impact to applications; • Frequent application failure, but no data loss; • Serious but predictable management system failure • Significant system performance degradation | | |
| | Severity Level 3 | | |
| | <ul style="list-style-type: none"> • Degradation of machine performance causing inconvenience to the business. • Covered Solution or System is up and running with limited or no significant impacts. | | |
| | Examples: | | |
| | <ul style="list-style-type: none"> • Bugs which cause limited or no direct impact to performance and functionality • Request to replace a bug work-around; • Limited impact defective functionality • System performance support questions and issues | | |
| | Severity Level 4 | | |

| Item # | TECHNICAL SPECIFICATIONS | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--------------------------------|----------------------------|--|--|--|-------------------|--|---|--|--|--|---|--|--|--|---|--|---|--|--|--|--------------------------------------|--|---|--|--|
| | <ul style="list-style-type: none"> • A minor event causing little or no impact to UCPBS business. <p>Examples:</p> <ul style="list-style-type: none"> • Scheduled activities agreed with UCPBS • Methods of Procedure (MOP) <p>Severity Level 5</p> <ul style="list-style-type: none"> • The call is undergoing ongoing monitoring, but no further action is required. <p>Examples:</p> <ul style="list-style-type: none"> • Requests for status updates on action taken/plans; Monitoring Reports/Feedback on action steps taken. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | <p>System Requirements</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Must support the following systems:</th><th style="text-align: left;">Statement of Compliance</th></tr> </thead> <tbody> <tr> <td>1. Operating System</td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later • Windows 8 Professional / Enterprise • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise • Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise </td><td></td></tr> <tr> <td>2. Servers</td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Small Business Server 2011 Essentials / Standard (64-bit) • Windows MultiPoint Server 2011 (64-bit); </td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later </td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Server 2012 Foundation / Essentials / Standard / Datacenter </td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter </td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Server 2016 Essentials / Standard / Datacenter; </td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Server 2019 Essentials / Standard / Datacenter; </td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Windows Server 2022. </td><td></td></tr> <tr> <td>3. Microsoft Terminal Servers</td><td></td></tr> <tr> <td> <ul style="list-style-type: none"> • Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1 </td><td></td></tr> </tbody> </table> | Must support the following systems: | Statement of Compliance | 1. Operating System | | <ul style="list-style-type: none"> • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later • Windows 8 Professional / Enterprise • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise • Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise | | 2. Servers | | <ul style="list-style-type: none"> • Windows Small Business Server 2011 Essentials / Standard (64-bit) • Windows MultiPoint Server 2011 (64-bit); | | <ul style="list-style-type: none"> • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later | | <ul style="list-style-type: none"> • Windows Server 2012 Foundation / Essentials / Standard / Datacenter | | <ul style="list-style-type: none"> • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter | | <ul style="list-style-type: none"> • Windows Server 2016 Essentials / Standard / Datacenter; | | <ul style="list-style-type: none"> • Windows Server 2019 Essentials / Standard / Datacenter; | | <ul style="list-style-type: none"> • Windows Server 2022. | | 3. Microsoft Terminal Servers | | <ul style="list-style-type: none"> • Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1 | | |
| Must support the following systems: | Statement of Compliance | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Operating System | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later • Windows 8 Professional / Enterprise • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise • Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Servers | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Small Business Server 2011 Essentials / Standard (64-bit) • Windows MultiPoint Server 2011 (64-bit); | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Server 2012 Foundation / Essentials / Standard / Datacenter | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Server 2016 Essentials / Standard / Datacenter; | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Server 2019 Essentials / Standard / Datacenter; | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Windows Server 2022. | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Microsoft Terminal Servers | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> • Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • Microsoft Remote Desktop Services based on Windows Server 2012 • Microsoft Remote Desktop Services based on Windows Server 2012 R2 • Microsoft Remote Desktop Services based on Windows Server 2016 • Microsoft Remote Desktop Services based on Windows Server 2019 • Microsoft Remote Desktop Services based on Windows Server 2022 |
| | <p>4. 32-bit Linux operating systems</p> <ul style="list-style-type: none"> • CentOS 6.7 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • Linux Mint 19 and later • Mageia 4 • Red Hat Enterprise Linux 6.7 and later • ALT Education 9 • ALT Workstation 9 |
| | <p>5. 64-bit Linux operating systems</p> <ul style="list-style-type: none"> • AlterOS 7.5 and later • Amazon Linux 2 • Astra Linux Common Edition (operational update 2.12). • Astra Linux Special Edition RUSB.10015-01 (operational update 1.5) • Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6) • CentOS 6.7 and later • CentOS 7.2 and later • CentOS 8.0 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • EulerOS V2.0SP2 2.2.17 • EulerOS V2.0SP5 2.5.6 • Linux Mint 19 and later • Linux Mint 20.1 and later • openSUSE Leap 15.0 and later • Oracle Linux 7.3 and later |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • Oracle Linux 8.0 and later • Pardus OS 19.1 • Red Hat Enterprise Linux 6.7 and later • Red Hat Enterprise Linux 7.2 and later • Red Hat Enterprise Linux 8.0 and later • SUSE Linux Enterprise Server 12 SP5 and later • SUSE Linux Enterprise Server 15 and later • Ubuntu 18.04 LTS and later • Ubuntu 20.04 LTS • ALT Education 9 • ALT Workstation 9 • ALT Server 9 • GosLinux 7.2 • Red OS 7.3 |
| | <p>6. MAC OS operating systems:</p> <ul style="list-style-type: none"> • macOS 10.14 – 12 |
| | <p>7. The proposed solution must support the following virtual platforms:</p> <ul style="list-style-type: none"> • VMware Workstation 16.2.3; • VMware ESXi 7.0 Update 3d; • Microsoft Hyper-V Server 2019; • Citrix Virtual Apps and Desktops 7 2203 LTSR; • Citrix Provisioning 2203 LTSR; • Citrix Hypervisor 8.2 LTSR (Cumulative Update 1). |
| | <p>8. The proposed solution must support protection of the latest Operating Systems versions across all platforms (Windows, Linux, MacOS, iOS, Android).</p> |
| | <p>9. The proposed solution must be able to detect following types of threat:</p> <ul style="list-style-type: none"> • Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software. |
| | <p>10. The proposed solution must support Anti-malware Scan Interface (AMSI).</p> |
| | <p>11. The proposed solution must have the ability to integrate with Windows Defender Security Center.</p> |
| | <p>12. The proposed solution must support Windows Linux subsystem.</p> |
| | <p>13. The proposed solution must provide next gen protection technologies. For example:</p> |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • protection against file-less threats • provision of multi-layered Machine Learning (ML) based protection and behavioral analysis during different stages of the kill-chain |
| | 14. The proposed solution must provide Memory Scanning for Windows workstations. |
| | 15. The proposed solution must provide Kernel Memory Scanning for Linux workstations. |
| | 16. The proposed solution must provide the ability to switch to cloud mode for threat protection, decreasing RAM and hard disk drive usage for resource-limited machines. |
| | 17. The proposed solution must have dedicated components to monitor, detect and block activities on Windows, Linux and Windows servers, and endpoints, to protect against remote encryption attacks. |
| | 18. The proposed solution must include signatureless components to detect threats even without frequent updates. Protection The proposed solution must be powered by Static ML for pre-execution and Dynamic ML for post-execution stages of the kill-chain on endpoints and in the cloud for Windows servers and workstations. |
| | 19. The proposed solution must provide behavioral analysis based on ML. |
| | 20. The proposed solution must provide the ability to integrate with the vendor's own Endpoint Detection and Response (EDR) and Anti-APT solutions, for active threat hunting and automated incident response. |
| | 21. The proposed solution must support integration with a standalone/independent automated threat detection and prevention sandbox solution that does not depend on the vendor's EDR and /or Anti-APT solution. |
| | 22. The proposed solution must include the ability to configure and manage firewall settings built into the Windows Server and Linux operating systems, through its management console. |
| | 23. The proposed solution must include the following components in a single agent installed on the endpoint: <ul style="list-style-type: none"> • Application, Web and Device Controls • Anomaly Detection • HIPS and Firewall • Patch Management |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <ul style="list-style-type: none"> • Encryption | |
| | <p>24. The proposed solution must provide Application and Device Controls for Windows workstations.</p> | |
| | <p>25. The proposed solution must include Application Launch/Start Control for the Windows Server operating system.</p> | |
| | <p>26. The proposed solution's protection for servers and workstations must include a dedicated component for protection against ransomware/cryptor virus activity on shared resources.</p> | |
| | <p>27. The proposed solution must, on detecting ransomware/cryptor-like activity, automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type.</p> | |
| | <p>28. The proposed solution must provide a pre-defined list of scan exclusions for Microsoft applications and services.</p> | |
| | <p>29. The proposed solution should support the installation of endpoint protection on servers without the need to restart.</p> | |
| | <p>30. The proposed solution must enable the following for endpoints:</p> <ul style="list-style-type: none"> • Manual Scanning • On-Access Scanning • On-Demand Scanning • Compressed File Scanning • Scan Individual File, Folder and Drive • Script Blocking and Scanning • Registry Guard • Buffer Overflow Protection • Background/Idle Scanning • Removable Drive Scanning on connection with system • The ability to detect and block untrusted hosts on detection of encryption-like activities on server shared resources. | |
| | <p>31. The proposed solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.</p> | |
| | <p>32. The proposed solution must have both local and global reputation databases.</p> | |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | 33. The proposed solution must be able to scan HTTPS, HTTP and FTP traffic against viruses and spyware, or any other malware. |
| | 34. The proposed solution must include a personal firewall capable, as an absolute minimum, of: <ul style="list-style-type: none"> • Blocking network activates of applications based on their categorization. • Blocking/allowing specific packets, protocols, IP addresses, ports and traffic direction. • The automatic and manual addition of network subnets, and modification of network activity permissions. |
| | 35. The proposed solution must prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization. |
| | 36. The proposed solution must be able to block network attacks and report the source of the infection. |
| | 37. The proposed solution must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files must be stored in a specific format that ensures they cannot pose any threat. |
| | 38. The proposed solution must have a proactive approach to preventing malware from exploiting existing vulnerabilities on servers and workstations. |
| | 39. The proposed solution must support AM-PPL (Anti-Malware Protected Process Light) technology for protection against malicious actions. |
| | 40. The proposed solution must include protection against attacks that exploit vulnerabilities in the ARP protocol in order to spoof the device MAC address. |
| | 41. The proposed solution must include a control component able to learn to recognize typical user behavior in a specific individual or group of protected computers, then identify and block anomalous and potentially harmful actions made by that endpoint or user. |
| | 42. The proposed solution must provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections. |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | 43. The proposed solution must include a dedicated component for scanning encrypted connections. |
| | 44. The proposed solution must be able to decrypt and scan network traffic transmitted over encrypted connections supported by the following protocols; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3. |
| | 45. The proposed solution must have the ability to automatically exclude web resources when a scan error occurs while performing an encrypted. |
| | 46. The proposed solution must include functionality to remotely wipe data on the endpoint (for workstations). |
| | 47. The proposed solution must have following remote data wipe functionalities: <ul style="list-style-type: none"> • In silent mode • On hard drives and removable drives • For all user accounts on the computer |
| | 48. The proposed solution's remote data wipe functionality must support the following modes: <ul style="list-style-type: none"> • Immediate data deletion • Postponed data deletion |
| | 49. The proposed solution's remote data wipe functionality must support the following data deletion methods: <ul style="list-style-type: none"> • Delete by using the operating resources - files are deleted but are not sent to the recycle bin • Delete completely, without recovery - making data practically impossible to restore after deletion. |
| | 50. The proposed solution must include functionality to automatically delete the data if there is no connection to the endpoint management server. |
| | 51. The proposed solution must support signature-based detection in addition to cloud-assisted and heuristics. |
| | 52. The proposed solution should have the ability to raise an alert on, clean, and delete a detected threat. |
| | 53. The proposed solution should have the ability to accelerate scanning tasks, skipping those objects that have not changed since the previous scan. |
| | 54. The proposed solution should have the ability to prioritize custom and on-demand scanning tasks for Linux workstations. |
| | 55. The proposed solution must allow the administrator to exclude specified files/ folders/applications/digital certificates from being scanned, either on-access (real-time protection) or during on-demand scans. |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|---|
| | 56. The proposed solution should include the functionality to isolate infected computers. |
| | 57. The proposed solution must automatically scan removable drives for malware when they are attached to any endpoint. Scan control should be based on drive size. |
| | 58. The proposed solution must be able to block the use of USB storage devices or allow access only to permitted devices, and allow read/write access only by domain users, to reduce data theft and enforce lock policies. |
| | 59. The proposed solution must be able to differentiate between USB storage devices, printers, mobiles and other peripherals. |
| | 60. The proposed solution must be able to log file operations (Write and Delete) on USB storage devices. This should not require any additional license or component to be installed on the endpoint. |
| | 61. The proposed solution must have ability to block the execution of any executable from the USB storage device. |
| | 62. The proposed solution must have ability to block/allow user access to web resources based on websites, content type, user and time of day. |
| | 63. The proposed solution must have a specific detection category to block website banners. |
| | 64. The proposed solution must provide the ability to configure Wi-Fi networks based on Network Name, Authentication Type, Encryption Type, so these can later be used to block or allow the Wi-Fi connections. |
| | 65. The proposed solution must support user-based policies for Device, Web and Application Control. |
| | 66. The proposed solution should specifically allow the blocking of the following devices: <ul style="list-style-type: none"> • Bluetooth • Mobile devices • External modems • CD/DVDs • Cameras and Scanners • MTPs • And the transfer of data to mobile devices |
| | 67. The proposed solution should feature cloud integration, to provide the fastest possible updates on malware and potential threats. |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | 68. The proposed solution must have ability to manage user access rights for Read and Write operations on CDs/DVDs, removable storage devices and MTP devices. |
| | 69. The proposed solution must feature firewall filtering by local address, physical interface, and packet Time-To-Live (TTL). |
| | 70. The proposed solution must allow the administrator to monitor the application's use of custom/random ports after it has launched. |
| | 71. The proposed solution must support the blocking of prohibited (Deny-List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-Lists. |
| | 72. The proposed solution must have a cloud-integrated Application Control component for immediate access to the latest updates on application ratings and categories. |
| | 73. The proposed solution must offer protection to files executed in Windows Server containers. |
| | 74. The proposed solution must include traffic malware filtering, web link verification and web-resource control based on cloud categories. |
| | 75. The proposed solution Web Control/Restriction component must include a Cryptocurrencies and Mining category. It must also include predefined regional legal restrictions to comply with Belgian and Japanese Law. |
| | 76. The proposed solution must have the ability to allow applications based on their digital signature certificates, MD5, SHA256, META Data, File Path, and pre-defined security categories. |
| | 77. The proposed solution must have controls for the download of DLL and Drivers. |
| | 78. The proposed solution's application control component must include Deny List and Allow List operational modes. |
| | 79. The proposed solution must support the control of scripts from PowerShell. |
| | 80. The proposed solution must support Test Mode with report generation on the launch of blocked applications. |
| | 81. The proposed solution must have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files "HIPS functionality". |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| 82. | The proposed solution must have the ability to control system/user application access to audio and video recording devices. |
| 83. | The proposed solution must provide a facility to check applications listed in each cloud-based category. |
| 84. | The proposed solution must have ability to integrate with a vendor-specific Advanced Threat Protection system. |
| 85. | The proposed solution must have ability to automatically regulate the activity of programs running, including access to the file system and registry as well as interaction with other programs. |
| 86. | The proposed solution must have the ability to automatically delete Application Control rules if an application is not launched during a specified interval. The interval must be configurable. |
| 87. | The proposed solution must have ability to automatically categorize applications launched prior to endpoint protection installation. |
| 88. | <p>The proposed solution must have endpoint mail threat protection with:</p> <ul style="list-style-type: none"> • Attachment filter and the ability to rename attachments. • Scanning of mail messages when receiving, reading and sending. |
| 89. | The proposed solution must have the ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays. |
| 90. | The proposed solution must enable the user of the computer to perform a check on a file's reputation from the File Context menu. |
| 91. | The proposed solution must include the scanning of all scripts, including those developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the internet. |
| 92. | The proposed solution must provide protection against as yet unknown malware based of the analysis of their behavior and examination of changes in the system register, together with a strong remediation engine to automatically restore any system changes made by the malware. |



| Item # | TECHNICAL SPECIFICATIONS |
|--|---|
| | 93. The proposed solution must provide protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks. |
| | 94. The proposed solution must include IPv6 protocol support. |
| | 95. The proposed solution must offer scanning of critical sections of the computer as a standalone task. |
| | 96. The proposed solution must incorporate Application Self-Protection technology: <ul style="list-style-type: none"> • protecting against unauthorized the remote management of an application service. • protecting access to application parameters by setting a password. • preventing the disabling of protection by malware, criminals or amateur users. |
| | 97. The proposed solution must offer the ability to choose which threat protection components to install. |
| | 98. The proposed solution must include the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc. |
| | 99. The proposed solution must include the anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files. |
| | 100. The proposed solution must protect against as yet unknown malware belonging to registered families, based on heuristic analysis. |
| | 101. The proposed solution must include multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry). |
| | 102. The proposed solution must allow the administrator to create a single installer with the required configuration, for use by non-IT literate users. |
| Mobile Device Management | |
| 1. The proposed solution should be able to protect or manage Android mobile devices: <ul style="list-style-type: none"> • Android 5-13 (excluding Go edition) | |
| 2. The proposed solution should be able to protect or manage iOS mobile devices: | |


 A handwritten signature in black ink, appearing to read "А. А." (A. A.) or similar initials.

| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <p>iOS mobile device management:</p> <ul style="list-style-type: none"> • iOS 10.0–15.0 or iPadOS 13–15 <p>iOS online protection:</p> <ul style="list-style-type: none"> • iOS 14.1 or later • iPadOS 14.1 or later |
| 3. | The proposed solution must support Huawei Mobile Services. |
| 4. | The proposed solution must enable protection of the smartphone file system and the interception and scanning of all incoming objects transferred through wireless connections (infrared port, Bluetooth), EMS and MMS, while synchronizing with the personal computer and uploading files through a browser. |
| 5. | The proposed solution must have the ability to block malicious sites designed to spread malicious code, and phishing websites designed to steal confidential user data and access the user's financial information. |
| 6. | The proposed solution must have the functionality to add a website excluded from the scan to an Allow List. |
| 7. | The proposed solution must include website filtering by categories and allow the administrator to restrict user access to specific categories (for example, gambling-related websites or social media categories). |
| 8. | The proposed solution must enable the administrator to obtain information about the operation of antivirus and web protection on the user's mobile device. |
| 9. | The proposed solution must have the functionality to detect the location of the mobile device location via GPS, and show this on Google Maps. |
| 10. | The proposed solution must enable the administrator to take a picture (Mugshot) from the front camera of the mobile when it's locked. |
| 11. | The proposed solution must have containerization capabilities for Android devices. |
| 12. | The proposed solution must have the functionality to remotely wipe the following from Android devices: <ul style="list-style-type: none"> • containerized data • corporate email accounts |
| 13. | The proposed solution must have the functionality to remotely wipe the following from iOS devices: <ul style="list-style-type: none"> • All installed configuration profiles |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|---|
| | <ul style="list-style-type: none"> • All provisioning profiles • The iOS MDM profile • Applications for which Remove and the iOS MDM profile check box have been selected | |
| | <p>14. The proposed solution must allow the encryption of all data on the device (including user account data, removable drives and apps, as well as email messages, SMS messages, contacts, photos, and other files). Access to encrypted data should only be possible on an unlocked device through a special key or device unlock password.</p> | |
| | <p>15. The proposed solution must offer controls to ensure that all devices comply with corporate security requirements. Compliance Control should be based on a set of rules which should include the following components:</p> <ul style="list-style-type: none"> • Device check criteria • Time period allocated for the user to fix the non-compliance • action that will be taken on the device if the user does not fix the non-compliance within the set time period • Ability to remediate non-compliant devices | |
| | <p>16. The proposed solution must have the functionality to detect and to notify the administrator about device hacks (e.g. rooting/jailbreak).</p> | |
| | <p>17. The proposed solution should enable management of the following device features:</p> <ul style="list-style-type: none"> • Memory cards and other removable drives • Device camera • Wi-Fi connections • Bluetooth connections • Infrared connection port • Wi-Fi access point activation • Remote desktop connection • Desktop synchronization • Configure Exchange Mailbox settings • Configure mailbox on iOS MDM devices • Configure Samsung KNOX containers. • Configure the settings of the Android for Work profile • Configure Email/Calendar/Contacts • Configure Media content restriction settings. • Configure proxy settings on the mobile device |  |

| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| | <ul style="list-style-type: none"> • Configure certificates and SCEP |
| | <p>18. The proposed solution should allow the configuration of a connection to AirPlay devices to enable the streaming of music, photos, and videos from the iOS MDM device to AirPlay devices.</p> |
| | <p>19. The proposed solution must support all the below deployment methods for the mobile agent:</p> <ul style="list-style-type: none"> • Google Play, Huawei App Gallery and Apple App Store <ul style="list-style-type: none"> • KNOX Mobile Enrollment portal • Standalone preconfigured installation packages |
| | <p>20. The proposed solution must allow the configuration of Access Point Names (APN) to connect a mobile device to data transfer services on a mobile network.</p> |
| | <p>21. The proposed solution must allow the PIN on a mobile device to be reset remotely.</p> |
| | <p>22. The proposed solution must include the option to enroll Android devices using 3rd party EMM systems:</p> <ul style="list-style-type: none"> • VMware AirWatch 9.3 or later • MobileIron 10.0 or later • IBM MaaS360 10.68 or later • Microsoft Intune 1908 or later <ul style="list-style-type: none"> • SOTI MobiControl 14.1.4 (1693) or later |
| | <p>23. The proposed solution must have the functionality to enforce the installation of a mandatory app on the device.</p> |
| | <p>24. The proposed solution must support user-initiated mobile agent deployment via:</p> <ul style="list-style-type: none"> • Google Play • Huawei App Gallery • Apple App Store |
| | <p>25. The proposed solution must be able to scan files opened on the device.</p> |
| | <p>26. The proposed solution must be able to scan programs installed from the device interface.</p> |
| | <p>27. The proposed solution must be able to scan file system objects on the device or on connected memory extension cards on request of the user or according to a schedule.</p> |
| | <p>28. The proposed solution must provide the reliable isolation of infected objects in a quarantine storage location.</p> |



| Item # | TECHNICAL SPECIFICATIONS | |
|-------------------|---|--|
| | 29. The proposed solution must feature the updating of antivirus databases used to search for malicious programs and deleting dangerous objects. | |
| | 30. The proposed solution must be able to scan mobile devices for malware and other unwanted objects on-demand and on-schedule and deal with them automatically. | |
| | 31. The proposed solution must be able to manage and monitor mobile devices from same console as that used to manage computers and servers. | |
| | 32. The proposed solution must provide Anti-Theft functionality, so that lost and/or displaced devices can be located, locked and wiped remotely. | |
| | 33. The proposed solution must provide the facility to block forbidden applications from being launched on the mobile device. | |
| | 34. The proposed solution must be able to remotely install and remove applications from iOS devices. | |
| | 35. The proposed solution must be able to enforce security settings, such as password restrictions and encryption, on mobile devices. | |
| | 36. The proposed solution must have the ability to push applications recommended/required by the administrator to the mobile phone. | |
| | 37. The proposed solution must include a subscription model. | |
| | 38. The proposed solution must protect from online threats on iOS devices. | |
| Encryption | Statement of Compliance | |
| | 1. The proposed solution must support encryption on multiple levels: <ul style="list-style-type: none"> • Full disk encryption – including system disk • File and folder encryption • Removable media encryption | |
| | BitLocker and MacOS Filevault2 Encryption Management | |
| | 2. The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows: <ul style="list-style-type: none"> • The encryption of files on local computer drives. • The creation of encryption lists of files by extension or group of extensions. | |
| | The creation of encryption lists of folders on local computer drives. | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <p>3. The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows the encryption of files on removable drives. This must include the ability to:</p> <ul style="list-style-type: none"> • Specify a default encryption rule by which the application applies the same action to all removable drives. <p>Configure encryption rules for files stored on individual removable drives.</p> | |
| | <p>4. The proposed solution must offer integrated File Level Encryption (FLE) functionality that supports several file encryption modes for removable drives:</p> <ul style="list-style-type: none"> • The encryption of all files stored on removable drives <p>The encryption of new files only as they are saved or created on removable drives.</p> | |
| | <p>5. The proposed solution must offer Integrated File Level Encryption (FLE) functionality that allows files on removable drives be encrypted in portable mode. It must allow access to encrypted files on removable drives that are connected to computers without encryption functionality.</p> | |
| | <p>6. The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows the encryption of all files that specific applications can create or modify, on both hard drives and removable drives.</p> | |
| | <p>7. The proposed solution must offer integrated File Level Encryption (FLE) functionality that enables the management of rules of application access to encrypted files, including defining of an encrypted file access rule for any application. It must enable the blocking of access to encrypted files, or the allowing of access to encrypted files as ciphertext only.</p> | |
| | <p>8. The proposed solution must offer the capability to restore encrypted devices if an encrypted hard drive or removable drive is corrupted.</p> | |
| | <p>9. The proposed solution must offer Integrated Full Disk Encryption (FDE) functionality for hard drives and removable drives. As with FLE, there must be the capability to specify a default encryption rule by which the application applies the same action to all removable</p> | |



| ITEM # | TECHNICAL SPECIFICATIONS |
|---------------|---|
| | drives, or to configure encryption rules for individual removable drives. |
| 10. | The proposed solution must offer an encryption module which is managed centrally on all computers, with ability to enforce encryption policies and modify/stop encryption settings. |
| 11. | The proposed solution must offer the ability to centrally monitor encryption status and to generate reports regarding encrypted computers/devices. |
| 12. | The proposed solution must offer encryption that is fully transparent to end users and has no adverse impact on system performance and usage. |
| 13. | The proposed solution must offer Full Disk Encryption that supports the central management of authorized users, including adding, removing and password reset. Only authorized users should have permission to boot the encrypted disk. |
| 14. | The proposed solution must have the facility to block application access to encrypted data if needed. |
| 15. | The proposed solution must support the automatic encryption of removable storage devices and must be able to prevent data being copied to unencrypted media. |
| 16. | The proposed solution must provide a facility for creating password-protected containers which can be used to exchange data with external users. |
| 17. | The proposed solution must provide a central location for encryption key storage, and multiple recovery options. |
| 18. | The proposed solution's administrator/management server must have the ability to decrypt all encrypted data, regardless of location and/or user. |
| 19. | The proposed solution must support both QWERTY and AZERTY keyboard layouts for pre-boot authorization. |
| 20. | The proposed solution must support pre-boot authorization for following devices: Safe Net eToken 4100, Gemalto IDPrime .NET (511), Rutoken ECP Flash. |
| 21. | The proposed solution must provide the functionality to manage/apply Microsoft Bit locker encryption. |
| 22. | The proposed solution must provide the functionality to customize Microsoft BitLocker encryption settings including: <ul style="list-style-type: none"> • Use of Trusted Platform Module and password settings. |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--------------------------------|
| | <ul style="list-style-type: none"> • Use of hardware encryption for workstations and software encryption if Hardware encryption not available. <p>Use of authentication requiring data input in a preboot environment, even if the platform does not have the capability for preboot input (for example, with touchscreen keyboards on tablets).</p> <p>23. The proposed solution must support Encryption on Microsoft Surface Tablets.</p> | |
| | Systems Management, vulnerability and patch management | Statement of Compliance |
| | <p>1. The proposed solution should include features to manage computers remotely, including:</p> <ul style="list-style-type: none"> • Remote installation of third-party software • Reporting on existing software and hardware • Monitoring for the installation of unauthorized software <p>Removal of unauthorized software</p> <p>2. The proposed solution should include patch management capabilities for Windows operating systems and for installed third-party applications.</p> <p>3. The proposed solution's patch management functionality should be fully automated, with ability to detect, download and push missing patches to endpoints.</p> <p>4. The proposed solution must provide the facility to select which patches are to be downloaded/pushed to endpoints, based on their criticality.</p> <p>5. The proposed solution must be able to detect existing vulnerabilities in operating systems and other installed applications, and then to respond by automatically downloading/pushing the necessary patches to endpoints.</p> <p>6. The proposed solution must provide comprehensive reports on discovered vulnerabilities and missing patches, as well as on endpoints and patch deployment status.</p> <p>7. The proposed solution should have the capability to push specific patches based on criticality or severity.</p> <p>8. The proposed solution management server must be configurable as an updates source for Microsoft Updates and third-party applications.</p> | |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | 9. The proposed solution must include the vulnerability advisory of application vendor as well as security vendor. |
| | 10. The proposed solution must enable the administrator to approve updates. |
| | 11. The proposed solution must be able to automatically identify missing patches on individual endpoints and push only which are needed/missing. |
| | 12. The proposed solution should support patch aggregation to minimize number of updates needed. |
| | 13. The proposed solution should notify the administrator of any patches missing from endpoints as soon as the relevant information is available. |
| | 14. The proposed solution should provide the facility to manage patching separately for operating systems and for third-party applications. |
| | 15. The proposed solution should provide the facility to fix existing vulnerabilities either on any endpoint or only on specific ones. |
| | 16. The proposed solution should provide the facility to automatically detect/install all previously missed patches which are required to apply selected patch (dependencies). |
| | 17. The proposed solution must support the automated distribution of patches and updates for 150+ applications. |
| | 18. The proposed solution must have patch testing mode support functionality, |
| | 19. The proposed solution must include dedicated fields that contain information about 'Exploit found for the vulnerability'. |
| | 20. The proposed solution must include dedicated fields that contain information about 'Threat found for the vulnerability'. |
| | 21. The proposed solution must allow the administrator to restrict device users' ability to apply Microsoft Updates themselves. |
| | 22. The proposed solution must allow the administrator to specify which updates can be installed by users. |
| | 23. The proposed solution must enable the administrator to view a list of updates and patches unrelated to client devices. |
| | 24. The proposed solution must support operating system deployment. |

| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | 25. The proposed solution must support Wake-on LAN and UEFI. |
| | 26. The proposed solution must have built-in remote desktop sharing functionality. All file operations performed on the remote endpoint during the session must be logged on the Management Server. |
| | 27. The proposed solution must be able to deliver vulnerability fixes to client computers without installing the updates. |
| | 28. The proposed solution must allow the administrator to choose Windows updates to install, after which the client device user can install only those updates allowed/selected by the administrator. |
| | 29. The proposed solution must inform the administrator about unrelated updates and patches on the client device. |
| | 30. The proposed solution must be configurable/assignable as an update source for Microsoft and third-party updates. |
| | 31. The proposed solution must allow the administrator to select the Microsoft product and languages for which updates are downloaded. |
| | 32. The proposed solution must be able to remotely push/deploy EXE, MSI, bat, cmd, MSP files, and allow the administrator to define the command line parameter for the remote installation. |
| | 33. The proposed solution must be able to remotely uninstall applications, not limited to incompatible Anti-Virus programs. |
| | 34. The proposed solution must allow the administrator to use single task/job and to define different vulnerability-fix rules or criteria for Microsoft and third-party applications updates. |
| | 35. The proposed solution must allow the administrator set up rules for Microsoft and Third-party patch/update installation: <ul style="list-style-type: none"> • Start installation at computer restart or shutdown. • Install the required general system prerequisites. • Allow the installation of new application versions during updates. |
| | Download updates to the device without installing them. |
| | 36. The proposed solution must have ability to test the installation of updates on a percentage of computers |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--------------------------------|
| | before application to all target computers. The administrator must be able to configure the number of test computers as a percentage, and the time allocated prior to full rollout in terms of hours. | |
| | 37. The proposed solution must enable the removal/uninstallation of specified application and operating system updates. | |
| | 38. The proposed solution management server must be able to send logs to SIEMs and SYSLOG servers. | |
| | 39. The proposed solution must be able to track third party application licenses and raise notifications of any potential violations. | |
| | 40. The proposed solution's reporting must contain CVE information. | |
| | Centralized administration, monitoring, and update software requirements | Statement of Compliance |
| | <p>1. The proposed solution must support installation on the following Operating Systems:</p> <p>Windows:</p> <ul style="list-style-type: none"> • Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit • Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit • Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit • Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Pro 19H1 32-bit/64-bit • Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit • Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit • Microsoft Windows 10 Education 19H1 32-bit/64-bit • Microsoft Windows 10 Pro 19H2 32-bit/64-bit • Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit • Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit • Microsoft Windows 10 Education 19H2 32-bit/64-bit | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <ul style="list-style-type: none"> • Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bit/64-bit <p>Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bit/64-bit</p> <ul style="list-style-type: none"> • Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 11 Home 64-bit • Microsoft Windows 11 Pro 64-bit • Microsoft Windows 11 Enterprise 64-bit • Microsoft Windows 11 Education 64-bit • Microsoft Windows 8.1 Pro 32-bit/64-bit • Microsoft Windows 8.1 Enterprise 32-bit/64-bit • Microsoft Windows 8 Pro 32-bit/64-bit • Microsoft Windows 8 Enterprise 32-bit/64-bit • Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <ul style="list-style-type: none"> • Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit • Windows Server 2008 R2 Standard with Service Pack 1 and higher 64-bit • Windows Server 2008 R2 with Service Pack 1 (all editions) 64-bit • Windows Server 2012 Server Core 64-bit • Windows Server 2012 Datacenter 64-bit • Windows Server 2012 Essentials 64-bit • Windows Server 2012 Foundation 64-bit • Windows Server 2012 Standard 64-bit • Windows Server 2012 R2 Server Core 64-bit • Windows Server 2012 R2 Datacenter 64-bit • Windows Server 2012 R2 Essentials 64-bit • Windows Server 2012 R2 Foundation 64-bit • Windows Server 2012 R2 Standard 64-bit • Windows Server 2016 Datacenter (LTSB) 64-bit Windows Server 2016 Standard (LTSB) 64-bit <ul style="list-style-type: none"> • Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit • Windows Server 2019 Standard 64-bit • Windows Server 2019 Datacenter 64-bit • Windows Server 2019 Core 64-bit • Windows Server 2022 Standard 64-bit • Windows Server 2022 Datacenter 64-bit • Windows Server 2022 Core 64-bit • Windows Storage Server 2012 64-bit • Windows Storage Server 2012 R2 64-bit • Windows Storage Server 2016 64-bit • Windows Storage Server 2019 64-bit Linux: <ul style="list-style-type: none"> • Debian GNU/Linux 11.x (Bullseye) 32-bit/64-bit • Debian GNU/Linux 10.x (Buster) 32-bit/64-bit • Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit • Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bit • CentOS 7.x 64-bit • Red Hat Enterprise Linux Server 8.x 64-bit • Red Hat Enterprise Linux Server 7.x 64-bit • SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit • Astra Linux Special Edition 1.7 (including the closed software environment mode and the mandatory mode) 64-bit • Astra Linux Special Edition 1.6 (including the closed software environment mode and the mandatory mode) 64-bit • Astra Linux Common Edition 2.12 64-bit • Alt Server 10 64-bit • Alt Server 9.2 64-bit • Alt 8 SP Server (LKNV.11100-01) 64-bit • Alt 8 SP Server (LKNV.11100-02) 64-bit • Alt 8 SP Server (LKNV.11100-03) 64-bit • Oracle Linux 7 64-bit • Oracle Linux 8 64-bit • RED OS 7.3 Server 64-bit • RED OS 7.3 Certified Edition 64-bit <p>2. The proposed solution must support the following database servers:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2012 Express 64-bit • Microsoft SQL Server 2014 Express 64-bit • Microsoft SQL Server 2016 Express 64-bit • Microsoft SQL Server 2017 Express 64-bit • Microsoft SQL Server 2019 Express 64-bit • Microsoft SQL Server 2014 (all editions) 64-bit • Microsoft SQL Server 2016 (all editions) 64-bit • Microsoft SQL Server 2017 (all editions) on Windows 64-bit • Microsoft SQL Server 2017 (all editions) on Linux 64-bit <ul style="list-style-type: none"> • Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions) • Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions) • Microsoft Azure SQL Database • All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms • MySQL 5.7 Community 32-bit/64-bit • MySQL Standard Edition 8.0 (release 8.0.20 and higher) 32-bit/64-bit • MySQL Enterprise Edition 8.0 (release 8.0.20 and higher) 32-bit/64-bit • MariaDB 10.5.x 32-bit/64-bit |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • MariaDB 10.4.x 32-bit/64-bit • MariaDB 10.3.22 and higher 32-bit/64-bit • MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine • MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine • MariaDB 10.1.30 and higher 32-bit/64-bit |
| | <p>3. The proposed solution must support the following virtual platforms:</p> <ul style="list-style-type: none"> • VMware vSphere 6.7 • VMware vSphere 7.0 • VMware Workstation 16 Pro • Microsoft Hyper-V Server 2012 64-bit • Microsoft Hyper-V Server 2012 R2 64-bit • Microsoft Hyper-V Server 2016 64-bit • Microsoft Hyper-V Server 2019 64-bit • Microsoft Hyper-V Server 2022 64-bit • Citrix XenServer 7.1 LTSR • Citrix XenServer 8.x • Parallels Desktop 17 • Oracle VM VirtualBox 6.x (Windows guest login only) |
| | <p>4. The proposed solution must enable the installation of anti-malware software from a single distribution package.</p> |
| | <p>5. The proposed solution must have customizable installation profiles depending on the number of protected nodes.</p> |
| | <p>6. The proposed solution must support IPv6 addresses.</p> |
| | <p>7. The proposed solution must support two-step verification (authentication).</p> |
| | <p>8. The proposed solution must have ability to read information from Active Directory to obtain data about computer accounts in the organization.</p> |
| | <p>9. The proposed solution must include a built-in web console for the management of the endpoints, which should not require any additional installation.</p> |
| | <p>10. The proposed solution's web management console should be straightforward to use and must support touch screen devices.</p> |
| | <p>11. The proposed solution must automatically distribute computer accounts by management group if new computers appear on the network. It must provide</p> |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | the ability to set the transfer rules according IP address, type of the operating system and location in Organizational Units of Active Directory. |
| | 12. The proposed solution must provide for the centralized installation, update and removal of anti-malware software, together with centralized configuration, administration, and the viewing of reports and statistical information about its operation. |
| | 13. The proposed solution must feature the centralized removal (manual and automatic) of incompatible applications from the administration center. |
| | 14. The proposed solution must provide flexible methods for anti-malware agent installation: RPC, GPO, an administration agent for remote installation and the option to create a standalone installation package for local installation. |
| | 15. The proposed solution must enable the remote installation of anti-malware software with the latest anti-malware databases. |
| | 16. The proposed solution must enable the automatic update of anti-malware software and anti-malware databases. |
| | 17. The proposed solution must have automatic search facilities for vulnerabilities in applications and in the operating system on protected machines. |
| | 18. The proposed solution must enable the management of a component prohibiting the installation and/or running of programs. |
| | 19. The proposed solution must enable the management of a component controlling work with external I/O devices. |
| | 20. The proposed solution must enable the management of a component controlling user activity on the internet. |
| | 21. The proposed solution must allow for the testing of downloaded updates by means of the centralized administration software prior to distributing them to client machines, and the delivery of updates to user workplaces immediately after receiving them. |
| | 22. The proposed solution must be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization platform or hypervisor. |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | 23. The proposed solution must enable the creation of a hierarchy of administration servers at an arbitrary level and the ability to centrally managing the entire hierarchy from the upper level. |
| | 24. The proposed solution must support Managed Services Mode for administration servers, so that logically isolated administration server instances can be set up for different users and user groups. |
| | 25. The proposed solution must give access to the anti-malware security vendor's cloud services via the administration server. |
| | 26. The proposed solution must include the automatic distribution of licenses on client computers. |
| | 27. The proposed solution must be able to perform inventories of software and hardware installed on user computers. |
| | 28. The proposed solution must have a notification mechanism to inform users about events in the installed anti-malware software and settings, and to distribute notifications about events via email. |
| | 29. The proposed solution must enable the centralized installation of third-party applications on all or selected computers. |
| | 30. The proposed solution must have the ability to specify any computer in the organization as a center for relaying updates and installation packages, in order to reduce the network load on the main administration server system. |
| | 31. The proposed solution must have the ability to specify any computer in the organization as a center for forwarding anti-malware agent events from the selected group of client computers to the centralized administration server, in order to reduce the network load on the main administration server system. |
| | 32. The proposed solution must be able to generate graphical reports for anti-malware software events, and data about the hardware and software inventory, licensing, etc. |
| | 33. The proposed solution must be able to export of reports to PDF and XML files. |
| | 34. The proposed solution must provide the centralized administration of backup storages and quarantine on |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | all network resources where the anti-malware software is installed. |
| | 35. The proposed solution must provide the creation of internal accounts to authenticate administrators on the administration server. |
| | 36. The proposed solution must provide the creation of an administration system backup copy with the help of integrated administration system tools. |
| | 37. The proposed solution must support Windows Failover Cluster. |
| | 38. The proposed solution must have a built-in clustering feature. |
| | 39. The proposed solution must include some form of system to control virus epidemics. |
| | 40. The proposed solution must include Role Based Access Control (RBAC), and this must allow restrictions to be replicated throughout the management servers in the hierarchy. |
| | 41. The proposed solution's management server must include pre-defined security roles for the Auditor, Supervisor and Security Officer. |
| | 42. The proposed solution must have ability manage mobile devices through remote commands. |
| | 43. The proposed solution must have ability to delete downloaded updates. |
| | 44. The proposed solution must generate Managing Administration Server updates from the application interface. |
| | 45. The proposed solution must enable the selection of an update agent for client computers based on a network analysis. |
| | 46. The proposed solution must clearly show information about the distribution of vulnerabilities across managed computers. |
| | 47. The proposed solution's management server interface must support the Arabic language. |
| | 48. The proposed solution's management server must maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed. |
| | 49. The proposed solution's management server must have functionality to create multiple profiles within a protection policy with different protection settings |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|---|
| | <p>that can be simultaneously active on a single/multiple devices based on the following activation rules:</p> <ul style="list-style-type: none"> • Device status • Tags • Active directory • Device owners • Hardware |
| | <p>50. The proposed solution must support following notification delivery channels:</p> <ul style="list-style-type: none"> • Email • Syslog • SMS • SIEM |
| | <p>51. The proposed solution must have the ability to define an IP address range, in order to limit client traffic towards the management server based on time and speed.</p> |
| | <p>52. The proposed solution must have the ability to perform inventory on scripts and .dll files.</p> |
| | <p>53. The proposed solution must have the ability to tag/mark computers based on:</p> <ul style="list-style-type: none"> • Network Attributes <ul style="list-style-type: none"> ◦ Name ◦ Domain and/or Domain Suffix ◦ IP address ◦ IP address to management server • Location in Active Directory <ul style="list-style-type: none"> ◦ Organizational Unit ◦ Group • Operating System <ul style="list-style-type: none"> ◦ Type and Version ◦ Architecture ◦ Service Pack number • Virtual Architecture • Application registry <ul style="list-style-type: none"> ◦ Application name ◦ Application version ◦ Manufacturer |
| | <p>54. The proposed solution must have the ability to create/define settings based on a computer's location</p> |



| Item # | TECHNICAL SPECIFICATIONS |
|---------------|--|
| | in the network, rather than the group to which it belongs in the management server. |
| | 55. The proposed solution must have the functionality to add a unidirectional connection mediator between the management server and the endpoint connecting over the internet/public network. |
| | 56. The proposed solution must allow the administrator to define restricted settings in policy/profile settings, so that a virus scan task can be triggered automatically when a certain number of viruses are detected over defined amount of time. The values for the number of viruses and timescale must be configurable. |
| | 57. The proposed solution must have a customizable dashboard generating and displaying real time statistics for endpoints. |
| | 58. The proposed solution must allow the administrator to customize reports. |
| | 59. The proposed solution must have the functionality to detect non-persistent virtual machines and automatically delete them and their related data from the management server when powered off. |
| | 60. The proposed solution must enable the administrator to set a period of time after which a computer not connected to the management server, and its related data are automatically deleted from the server. |
| | 61. The proposed solution must allow the administrator to create categories/groups of application based on: <ul style="list-style-type: none"> • Application Name • Application Path • Application Metadata • Application Digital certificate • Vendor pre-defined application categories • SHA • Reference computers to allow/deny their execution on endpoints. |
| | 62. The proposed solution must allow the administrator to define different status change conditions for groups of endpoints in the management server. |
| | 63. The proposed solution must allow the administrator to add custom/3rd party endpoint management tools into the management server. |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <p>64. The proposed solution must have a built-in feature/module to remotely collect the data needed for troubleshooting from the endpoints, without requiring physical access.</p> | |
| | <p>65. The proposed solution must allow the administrator to create a Connection Tunnel between a remote client device and the management server if the port used for connection to the management server is not available on the device.</p> | |
| | <p>66. Suggest solution must have built-in functionality to remotely connect to the endpoint using Windows Desktop Sharing Technology. In addition, the solution must be able to maintain the auditing of administrator actions during the session.</p> | |
| | <p>67. The proposed solution must have a feature to create a structure of administration groups using the Groups hierarchy, based on the following data:</p> <ul style="list-style-type: none"> • structures of Windows domains and workgroups • structures of Active Directory groups • contents of a text file created by the administrator manually | |
| | <p>68. The proposed solution must be able to retrieve information about the equipment detected during a network poll. The resulting inventory should cover all equipment connected to the organization's network.</p> <p>Information about the equipment should update after each new network poll. The list of detected equipment should cover the following:</p> <ul style="list-style-type: none"> • devices • mobile devices • network devices • virtual devices • OEM components • computer peripherals • connected devices • VoIP phones • network repositories <p>The administrator must be able to add new devices to the equipment list manually or edit information about equipment that already exists on the network.</p> | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| | 'Device is Written Off' functionality must be available, so that such devices are not displayed in the equipment list. |
| | 69. The proposed solution must incorporate a single distribution/relay agent to support at least 10,000 endpoints for the delivery of protection, updates, patches, and installation packages to remote sites. |
| | 70. The proposed solution must incorporate a single distribution/relay agent to relay/transfer or proxy threat reputation requests from endpoints to the management server. |
| | 71. The proposed solution must support the download of differential files rather than full update packages. |
| | 72. The proposed solution must support OPEN API, and include guidelines for integration with 3rd party external systems. |
| | 73. The proposed solution must include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer. |
| | 74. The proposed solution must include Role Based Access Control (RBAC) with customizable predefined roles. |
| | 75. The proposed solution's primary/parent management server must be able to relay updates and cloud reputation services. |
| | 76. The proposed solution's reports must include information about each threat and the technology that detected it. |
| | 77. The proposed solution report must include details about which endpoint protection components are, or are not, installed on client devices, regardless of the protection profile applied/existing for these devices. |
| | 78. The proposed solution's primary management server must be able to retrieve detailed information reporting on the health status etc. of managed endpoints from the secondary management servers. |
| | 79. The proposed solution must include the option for the customer to either deploy an on-premises management console, or use the vendor-provided cloud-based management console. |
| | 80. The proposed solution must be able to integrate with the vendor's cloud-based management console for endpoint management at no additional cost. |



| Item # | TECHNICAL SPECIFICATIONS | |
|---|---------------------------------|--------------------------------|
| | | |
| 81. The proposed solution must enable swift migration from the on-premises management console to the vendor cloud-based management console. | | |
| 82. The proposed solution must include the following SIEM integration options: <ul style="list-style-type: none"> • HP (Microfocus) ArcSight • IBM QRadar • Splunk • Syslog | | |
| 83. The proposed solution must include support for cloud-based deployment via: <ul style="list-style-type: none"> • Amazon Web Services • Microsoft Azure | | |
| 84. The proposed solution must provide anti-malware database update mechanisms including: <ul style="list-style-type: none"> • Multiple ways of updating, including global communication channels over the HTTPS protocol, shared resource at local network and removable media. • Verification of the integrity and authenticity of updates by means of an electronic digital signature. | | |
| 85. The proposed solution must support Single Sign On (SSO) using NTLM and Kerberos. | | |
| 86. The solution must be capable of removing the existing endpoint security agent/solution within 8 hours without user intervention, i.e., auto-discover on 300 devices. (As applicable) | | |
| 87. The solution must be capable of deploying and installing the endpoint security agents within 8 hours without user intervention, i.e., auto-discover on 300 devices. (As applicable) | | |
| 88. The solution must be fully operational within 1 hour after deployment and installation to each device. (As applicable) | | |
| Documentation | | Statement of Compliance |
| 1. Requirements for solution documentation. Documentation for all anti-malware software, including administration tools, should include the following documents: Online Help for Administrators Online Help for implementation best practices | | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--|---|--|
| | <p>2. The anti-malware software documentation provided should describe in detail the processes of installation, configuration and use of the anti-malware software.</p> | |
| 11 General Terms and Conditions | | |
| <p>A. Terms</p> <p>1. The request(s) for payment shall be made to UCPBS in writing, accompanied by an invoice describing, as appropriate, the output/report delivered and/or services performed, and by submission of other required documents and obligations stipulated in this contract.</p> <p>2. All payments shall be VAT-inclusive and subject to 2% expanded withholding tax and 5% Final VAT (if supplier is VAT-registered with BIR).</p> <p>3. Since the payment/s shall be subject to the usual government accounting and auditing requirements, the Supplier is expected to be familiar with the Government Accounting and Auditing Manual (GAAM).</p> <p>4. Retention Payment.</p> <p>A retention payment of one (1) percent shall be withheld by UCPBS. It shall be based on the total amount due to the Supplier prior to any deduction and shall be retained from every progress payment.</p> <p>The total 'retention money' shall be due for release upon approval/ acceptance of the Final Report/Acceptance. The Supplier may, however, request the substitution of the retention money for each progress billing with irrevocable standby letters of credit from a commercial bank, bank guarantees, or surety bonds callable on demand, of amounts equivalent to the retention money substituted for and acceptable to UCPBS provided that the Project is on schedule and is satisfactorily undertaken. Otherwise, the one (1) percent retention shall be made. Said irrevocable standby letters of credit, bank guarantees and/or surety bonds, to be posted in favor of UCPBS shall be valid for the duration of the contract.</p> <p>B. Warranties</p> <p>Warranty on Parts</p> <p>The Supplier warrants that the replacement part as specified under Technical Specifications Section 5 (Support Coverage) will be free from defects in material or workmanship for a period of three (3) months from the date the part was installed on the covered component detailed in Technical Specifications Section 3 (Covered Components).</p>  | | |

| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| | <p>Warranty on Services The Supplier warrants that the activities included in the Solution will be executed using the degree of skill and care required by customarily accepted good professional and technical practices. If the services provided did not conform to the terms and conditions specified under this TOR, the Supplier shall re-perform such services at no additional cost to the Bank.</p> <p>C. Incidental Services (Indicate, if any)</p> <ol style="list-style-type: none"> 1. Incidental Services, if any, shall be as described in Technical Specs. 2. Such incidental services may include the following: Project/ Solution documentation, knowledge transfer (trainings), systems and tools to facilitate monitoring of Project/Solution tasks, trouble tickets, incident reports, and inventory. <p>D. Termination</p> <p>UCPBS may, subject to five (5) days' advance notice, terminate the contract with the Supplier or cancel the purchase order (PO) it issued to the Supplier, on any of the following grounds:</p> <ol style="list-style-type: none"> 1. Misrepresentation by the selected supplier of any matter which UCPBS deems material, or 2. Failure by the selected supplier to deliver the goods and services to the satisfaction of UCPBS on the Delivery Schedule. <p>Notwithstanding any provision in the General and Special Conditions of Contract, UCPBS may pre-terminate this Contract subject to a notice to the Supplier within thirty (30) days prior to the effective date of pre-termination.</p> <p>E. Liquidated Damages</p> <p>When the supplier fails to satisfactorily deliver goods and/or services under this Terms of Reference (TOR) within the specified delivery schedule, inclusive of duly granted time extension, if any, the supplier shall be liable for damages in an amount equal to one-tenth (1/10) of one percent (1%) of the contract price the for delivery for every day of delay until such goods are finally delivered and accepted by UCPBS. Such amount shall be deducted from any money due or which may become due to the Supplier.</p> <p>If UCPBS opts to terminate the contact or cancel the PO, the Supplier shall be liable to pay UCPBS liquidated damages in an amount computed, as follows:</p> <p class="list-item-l1">(a) In case of misrepresentation, one-tenth (1/10) of one percent (1%) of the contract price per day starting from the date of UCPBS discovery of the misrepresentation until the effective date of termination of the contract or cancellation of the PO, and/or</p> |



| Item # | TECHNICAL SPECIFICATIONS |
|-----------|---|
| | <p>(b) In case of delay in the delivery of the goods and/or services to the satisfaction of UCPBS, one-tenth (1/10) pf one percent (1%) of the contract price per day starting from the Delivery schedule until the effective date of termination of the contract or cancellation of the PO.</p> <p>In case the selected supplier is guilty of both misrepresentation and delay, the liquidated damages shall be computed using the formula of either (a) or (b), whichever is higher. The Supplier shall pay UCPBS the liquidated damages under this Section within five (5) days from the effective date of the termination of the contract or cancellation of the PO without need of demand.</p> <p>F. No Employer-Employee Relationship</p> <p>Nothing in this TOR shall be construed as constituting an employer and employee relationship between UCPBS and the selected supplier, his/her/its employees and/or representatives.</p> <p>G. Confidentiality of Information</p> <p>The selected supplier shall observe the provisions of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, in the performance of its obligations under this TOR.</p>  |

Section VIII. Checklist of Technical and Financial Documents

A handwritten signature consisting of two loops at the top and a diagonal line with a small hook at the bottom right.

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

- (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages) in accordance with Section 8.5.2 of the IRR;
- Or**
- (b) Registration certificate from Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for cooperatives or its equivalent document,
- And**
- (c) Mayor's or Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the equivalent document for Exclusive Economic Zones or Areas;
- And**
- (d) Tax clearance per E.O. No.398, s, 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).

Technical Documents

- (e) Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; **and**
- (f) Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 revised IRR of RA No. 9184, within the relevant period as provided in the Bidding Documents; **and**
- (g) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;
- or**
- (h) Original copy of Notarized Bid Securing Declaration; **and**
- (i) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, if applicable; **and**
- (j) Original duly signed Omnibus Sworn Statement (OSS); **and** if applicable, Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

Financial Documents



- (j) The Supplier's audited financial statements, showing, among others, the Supplier's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission; **and**
- (k) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);
or
A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

Class "B" Documents

- (l) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;
or
duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

II. FINANCIAL COMPONENT ENVELOPE

- (m) Original of duly signed and accomplished Financial Bid Form; **and**
- (n) Original of duly signed and accomplished Price Schedule(s).

Other documentary requirements under RA No. 9184 (as applicable)

- (o) [For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos] Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
- (p) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

Section IX. Bidding Forms

A handwritten signature or mark consisting of a stylized circle and a line extending downwards and to the right.

Bid Form# _____ Bid Form

BID FORM

Date : _____
Project Identification No. : _____

To: [name and address of Procuring Entity]

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers [*insert numbers*], the receipt of which is hereby duly acknowledged, we, the undersigned, offer to [*supply/deliver/perform*] [*description of the Goods*] in conformity with the said PBDs for the sum of [*total Bid amount in words and figures*] or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: [*specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties*], which are itemized herein or in the Price Schedules,

If our Bid is accepted, we undertake:

- a. to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);
- b. to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;
- c. to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

[Insert this paragraph if Foreign-Assisted Project with the Development Partner:

Commissions or gratuities, if any, paid or to be paid by us to agents relating to this Bid, and to contract execution if we are awarded the contract, are listed below:

Name and address Amount and Purpose of
of agent Currency Commission or gratuity

(if none, state "None")]

Until a formal Contract is prepared and executed, this Bid, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the Lowest Calculated Bid or any Bid you may receive.



We certify/confirm that we comply with the eligibility requirements pursuant to the PBDs.

The undersigned is authorized to submit the bid on behalf of *[name of the bidder]* as evidenced by the attached *[state the written authority]*.

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Name: _____

Legal capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

A handwritten signature is located in the bottom right corner of the page.

Bid Form# ____ Contract Agreement Form

CONTRACT AGREEMENT

THIS AGREEMENT made the _____ day of _____ 20____ between [name of PROCURING ENTITY] of the Philippines (hereinafter called "the Entity") of the one part and [name of Supplier] of [city and country of Supplier] (hereinafter called "the Supplier") of the other part;

WHEREAS, the Entity invited Bids for certain goods and ancillary services, particularly [brief description of goods and services] and has accepted a Bid by the Supplier for the supply of those goods and services in the sum of [*contract price in words and figures in specified currency*] (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.
2. The following documents as required by the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of this Agreement, *viz.:*
 - i. Philippine Bidding Documents (PBDs);
 - i. Schedule of Requirements;
 - ii. Technical Specifications;
 - iii. General and Special Conditions of Contract; and
 - iv. Supplemental or Bid Bulletins, if any
 - ii. Winning bidder's bid, including the Eligibility requirements, Technical and Financial Proposals, and all other documents or statements submitted;
 - iii. Bid form, including all the documents/statements contained in the Bidder's bidding envelopes, as annexes, and all other documents submitted (*e.g.*, Bidder's response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;
 - iv. Performance Security;
 - iv. Notice of Award of Contract; and the Bidder's conforme thereto; and
 - v. Other contract documents that may be required by existing laws and/or the Procuring Entity concerned in the PBDs. **Winning bidder agrees that additional contract documents or information prescribed by the GPPB that are subsequently required for submission after the contract execution, such as the Notice to Proceed, Variation Orders, and**

Warranty Security, shall likewise form part of the Contract.

3. In consideration for the sum of [*total contract price in words and figures*] or such other sums as may be ascertained, [*Named of the bidder*] agrees to [*state the object of the contract*] in accordance with his/her/its Bid.
4. The [*Name of the procuring entity*] agrees to pay the above-mentioned sum in accordance with the terms of the Bidding.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.

[*Insert Name and Signature*]

[*Insert Name and Signature*]

[*Insert Signatory's Legal Capacity*]

[*Insert Signatory's Legal Capacity*]

for:

for:

[*Insert Procuring Entity*]

[*Insert Name of Supplier*]

Acknowledgment

[*Format shall be based on the latest Rules on Notarial Practice*]



Bid Form# _____ Omnibus Sworn Statement

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. [Select one, delete the other:]

[If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

[If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. [Select one, delete the other:]

[If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

[If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable);];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;
4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;
5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. [Select one, delete the rest:]

[If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a partnership or cooperative:] None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

[If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and
8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:
 - a. Carefully examining all of the Bidding Documents;
 - b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
 - c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
 - d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.
9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this _____ day of _____, 20____ at _____, Philippines.

*[Insert NAME OF BIDDER OR ITS AUTHORIZED
REPRESENTATIVE]*

*[Insert signatory's legal capacity]
Affiant*

Jurat

[Format shall be based on the latest Rules on Notarial Practice]

A handwritten signature is located in the bottom right corner of the page.

Bid Form# _____ Secretary's Certificate

I, _____, a duly elected and qualified Corporate Secretary of [Name of Bidder], a corporation duly organized and existing under and by virtue of the law of the PHILIPPINES, DO HERBY CERTIFY that:

I am familiar with the facts herein certified and duly authorized to certify the same:

At the meeting of the Board of Directors of the Corporation duly convened and held on _____ at which meeting a quorum was present and acting throughout, the following resolutions were approved, and the same have not been annulled, revoked and amended in any way whatever and rare in full force and effect on the date hereof:

"RESOLVED, that (Name of Bidder), as it hereby is/are, authorized to participate in the bidding of (Name of the Project), and that if awarded the project shall enter into a contract with the UCPB Savings, Inc.; and in connection therewith hereby appoint (Name of Representative/s), acting as duly authorized and designated representatives of [Name of Bidder], is/are granted full power and authority to do effectively as the (Designation of the Representative/s) might do if personally present with full power of substitution and revocation and hereby satisfying and confirming all that my said representative shall lawfully do or cause to be done by virtue hereof;

| Name of Representatives | Designation | Specimen Signature |
|-------------------------|-------------|--------------------|
| _____ | _____ | _____ |
| _____ | _____ | _____ |
| _____ | _____ | _____ |

RESOLVED FURTHER THAT, the [Name of Bidder] hereby authorizes its representative/s to:

1. Execute a waiver of jurisdiction whereby the [Name of Bidder] hereby submits itself to the jurisdiction of the Philippine government and hereby waives its right to question the jurisdiction of the Philippine courts;
2. Execute a waiver that the [Name of Bidder] shall not seek and obtain writ of injunctions or prohibition or restraining order against the UCPB Savings, Inc. (UCPBS) or any other agency in connection with this project to prevent and restrain the bidding procedures related thereto, the negotiating of and award of a contract to a successful bidder, and the carrying out of the awarded contract.

IN WITHNESS WHEREOF, I have hereunto set my hand this _____ at _____, Philippines.

CORPORATE SECRETARY

SUBSCRIBED AND SWORN to before me this _____ at
_____, Metro Manila, affiant exhibiting to me his respective [Government Issued ID]
with expiry date on _____.

NOTARY PUBLIC

Doc. No. _____

Page No. _____

Book No. _____

Series of 2022

Bid Form# _____ Bid Securing Declaration Form

REPUBLIC OF THE PHILIPPINES)
CITY OF _____) S.S.

BID SECURING DECLARATION
Project Identification No.: [Insert number]

To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid Securing Declaration.
2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f), of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.
3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:
 - a. Upon expiration of the bid validity period, or any extension thereof pursuant to your request;
 - b. I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and
 - c. I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this _____ day of [month] [year] at [place of execution].

[Insert NAME OF BIDDER OR ITS AUTHORIZED
REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Bid Form# _____ **Statement of all Ongoing Contracts**

**Statement of all Ongoing Government and Private Contracts Including Contracts
Awarded but not yet Started**

Business Name : _____

Business Address : _____

Note: This statement will be verified during the Post Qualification Stage through any of the following evidence not limited to:

Notice of Award and/or Contract/ Purchase Order

Official Receipt/ Sales Invoice

Notice to Proceed issued by the owner

Certificate of Accomplishment signed by the owner or authorized representative

Verification with the clients

Signature over printed name of Company Authorized Representative

Name and Designation (in print)

Date

Bid Form# _____ Statement of Single Largest Completed Contract

Statement of Single Largest Completed Contract Similar to the Contract to be Bid

This is to certify that (Company) has following completed contracts for the period of CY 2019 – 2022

| Date of the Contract | Contracting Party | Name of Contract | Amount of Contract | Date of Delivery/ End-User's Acceptance | Date of Official Receipt |
|----------------------|-------------------|------------------|--------------------|---|--------------------------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Note: This statement will be verified during the Post Qualification Stage through any of the following evidence not limited to:

Notice of Award and/or Contract/ Purchase Order

Official Receipt/ Sales Invoice

Notice to Proceed issued by the owner

Certificate of Accomplishment signed by the owner or authorized representative

Verification with the clients

Signature over printed name of Company Authorized Representative

Name and Designation (in print)

Date



Bid Form# _____ Net Financial Contracting Capacity Statement

NET FINANCIAL CONTRACTING CAPACITY (NFCC) STATEMENT

Summary of the bidder assets and liabilities on the basis of the income tax return and audited financial statement stamped "RECEIVED" by the Bureau of Internal Revenue or BIR authorized collection agent, for the immediately preceding year. The computation of its Net Financial Contracting Capacity (NFCC), which must be at least equal to the ABC to be bid, calculated as follows:

NFCC = [(Current assets minus current liabilities) (15)] minus the value of all outstanding or uncompleted portions of the project under ongoing contracts, including awarded contracts yet to be started coinciding with the contract to be bid.

| | Amount |
|---------------------------------------|--------|
| Current Assets | |
| Minus: Current Liabilities | |
| Sub-total | |
| Multiplied by 15 | |
| Sub-total | |
| Minus: Value of outstanding contracts | |
| NCFF | |

Signature over printed name of Company Authorized Representative

Name and Designation (in print)

Date



Bid Form# _____ Section VI. Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

| Item Number | Description | Quantity | Total | Delivered, Weeks/Months |
|--------------------|---|-----------------|--------------|--|
| 1 | Certificate of Entitlement / Proof of Support (Service Maintenance) | 1 | 1 | Within 1 week from the effective date of the contract and upon issuance of NTP. |
| 2 | License Certificate | 720 | 720 | Within 1 month from the effective date of the contract and upon issuance of NTP. |

I hereby commit to comply and deliver the above requirements.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date



Bid Form# _____ Section VII. Technical Specifications

STATEMENT OF COMPLIANCE TO TECHNICAL SPECIFICATIONS

INSTRUCTIONS:

The bidder must state in the last column opposite each parameter and required specifications either "Comply" or "Not Comply". All pages shall be properly signed. Bidders must state here either "Comply or " Not Comply" against each individual parameters of each requirements. Statements of "Comply or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance of the supporting evidence that is found to be false either during Bid Evaluation, post evaluation, or the execution of the Contract may be regarded as fraudulent and render the Bidder or Supplier liable for prosecution subject to the provisions of ITB Clause 3.1(a)(ii) and/or GCC Clause 2.1(a)(ii).

Technical Specifications

*Procurement of 720 Licenses and Support Maintenance for Endpoint Security
(ITB-ITD-007-25-04-2023)*

| Item # | TECHNICAL SPECIFICATIONS | |
|---------------|---|--------------------------------|
| | General Requirements | |
| 1 | The IT services to be rendered by Supplier to UCPBS shall be technical support and maintenance services defined as: 1 Any task or activity done by Supplier through electronic mail, telephone, messaging platforms (e.g. Viber, WhatsApp) or on-site presence, for the purpose of providing technical support, hardware and software maintenance, or assistance to UCPBS to troubleshoot, configure, update and check the performance of the Solution | |
| 2 | Technical Support and/or assistance shall include; the provision of analysis and recommendations and the performance or fulfillment of the recommendation/s. | |
| 3 | Technical Support Services shall be available from Mondays through Sundays, 24x7 (working-hours and non-working hours). | |
| 4 | Location/s of Covered Components: 1. 2 nd floor, Overseas Filipino (OF) Bank Center Building, 1000 Liwasang Bonifacio, Intramuros, Barangay 656-A, 1000 Manila City, Philippines; 2. 2 nd floor, UCPBS Disaster Recovery Site, 721 Aurora Blvd., Quezon City, Philippines | |
| 5 | Scope of Local Support Services | Statement of Compliance |
| | a. The Supplier, through a Service or Help Desk, shall provide technical support assistance by electronic mail, telephone, and messaging platforms. | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <p>b. The Supplier's Service Desk shall be staffed with technically competent support engineers. The Service Desk shall be the single point-of-contact for UCPBS for Local Support Services.</p> <p>c. Service Desk operations shall be supported by the Supplier's internal electronic ticketing system, along with the necessary electronic mail and telephony systems.</p> <p>d. For support requests that cannot be resolved remotely, On-site support shall be provided by Supplier</p> | |
| 6 | <p>Support Level</p> <p>Supplier shall directly provide Levels 1 and 2 Technical Support to UCPBS's support requests. These Levels are defined as:</p> <ul style="list-style-type: none"> • Level 1 Technical Support – First-line support involving the tasks of problem identification, understanding UCPBS's expectations, initial problem diagnosis, and basic technical troubleshooting based on Supplier's knowledgebase of known problems and resolutions. • Level 2 Technical Support – Advanced Support involving the tasks of complex problem identification, in-depth problem diagnosis, and advanced technical troubleshooting. In some cases, if necessary, reproduction of the problem by Supplier, in coordination with UCPBS, is necessary to arrive at a solution. <p>Supplier shall facilitate resolution of support requests requiring Levels 3 and 4 support involving 3rd party supplier(s), including the Manufacturers-Principals, who developed and who have intellectual property rights over the Solution. These levels are defined as:</p> <ul style="list-style-type: none"> • Level 3 Technical Support – Support of this nature will require the involvement of the 3rd party supplier to conduct research and development to a new and/or unknown issue. Such issues shall require solutions such as bug fix, error correction, custom engineering or interim patch or fix for the Solution to operate as required by UCPBS, which only the 3rd Party supplier may provide. • Level 4 Technical Support – Support of this nature will involve the 3rd Party supplier's integration of the resolution to the Solution as an official patch, feature or capability. <p>Regardless of Support Level, UCPBS's concerns, incidents and queries may be referred to the 3rd Party supplier from whom the supported Solution originated without any additional cost to UCPBS.</p> | |
| 7 | <p>Service Management and Reporting</p> <ul style="list-style-type: none"> • Supplier shall handle and manage UCPBS's service requests in accordance with workflow procedures approved by UCPBS. • Quarterly reports on support requests and reported incidents will be completed by Supplier and submitted to UCPBS. | |



| Item # | TECHNICAL SPECIFICATIONS | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------------|---|------------------------|----------------|--------------------|------------------------|--|---|---------|---------|--|---|---------|---------|--|---|---------|--------|--|---|---------|--------|--|---|-------|------|--|--|
| | <ul style="list-style-type: none"> Quarterly status reports will be discussed by the Supplier Account Service Manager with UCPBS to ensure that UCPBS is aware of possible support issues and risks faced by UCPBS. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | Service Level Agreement <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Severity Level</th> <th style="text-align: center;">Max. Response Time</th> <th style="text-align: center;">Max. Time Until Onsite</th> <th style="width: 10%;"></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td><td style="text-align: center;">2 Hours</td><td style="text-align: center;">4 Hours</td><td></td></tr> <tr> <td style="text-align: center;">2</td><td style="text-align: center;">3 Hours</td><td style="text-align: center;">8 Hours</td><td></td></tr> <tr> <td style="text-align: center;">3</td><td style="text-align: center;">4 Hours</td><td style="text-align: center;">2 Days</td><td></td></tr> <tr> <td style="text-align: center;">4</td><td style="text-align: center;">6 Hours</td><td style="text-align: center;">4 Days</td><td></td></tr> <tr> <td style="text-align: center;">5</td><td style="text-align: center;">1 Day</td><td style="text-align: center;">N.A.</td><td></td></tr> </tbody> </table> | | Severity Level | Max. Response Time | Max. Time Until Onsite | | 1 | 2 Hours | 4 Hours | | 2 | 3 Hours | 8 Hours | | 3 | 4 Hours | 2 Days | | 4 | 6 Hours | 4 Days | | 5 | 1 Day | N.A. | | |
| Severity Level | Max. Response Time | Max. Time Until Onsite | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 2 Hours | 4 Hours | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 3 Hours | 8 Hours | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 4 Hours | 2 Days | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 6 Hours | 4 Days | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | 1 Day | N.A. | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <p>Severity Level 1</p> <ul style="list-style-type: none"> Failure which causes major impact to UCPBS Business Covered Solution or System is not operational. <p>Examples:</p> <ul style="list-style-type: none"> System Hang (unable to save work in progress) System functionality failure causes data losses or system unusable; System down Functionality failure renders system ineffective <p>Severity Level 2</p> <ul style="list-style-type: none"> Failure causing severe degradation of UCPBS business Covered Solution or System is not operating with full capability but is still operational. <p>Examples:</p> <ul style="list-style-type: none"> Impaired or broken functionality with significant impact to applications; Frequent application failure, but no data loss; Serious but predictable management system failure Significant system performance degradation <p>Severity Level 3</p> <ul style="list-style-type: none"> Degradation of machine performance causing inconvenience to the business. Covered Solution or System is up and running with limited or no significant impacts. <p>Examples:</p> <ul style="list-style-type: none"> Bugs which cause limited or no direct impact to performance and functionality Request to replace a bug work-around; | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <ul style="list-style-type: none"> • Limited impact defective functionality • System performance support questions and issues <p>Severity Level 4</p> <ul style="list-style-type: none"> • A minor event causing little or no impact to UCPBS business. <p>Examples:</p> <ul style="list-style-type: none"> • Scheduled activities agreed with UCPBS • Methods of Procedure (MOP) <p>Severity Level 5</p> <ul style="list-style-type: none"> • The call is undergoing ongoing monitoring, but no further action is required. <p>Examples:</p> <ul style="list-style-type: none"> • Requests for status updates on action taken/plans; Monitoring Reports/Feedback on action steps taken. | |

| # | TECHNICAL SPECIFICATIONS | |
|---|---|---------------------------------------|
| | General Requirements | |
| | The IT services to be rendered by Supplier to UCPBS shall be technical support and maintenance services defined as: | |
| 1 | Any task or activity done by Supplier through electronic mail, telephone, messaging platforms (e.g., Viber, WhatsApp) or on-site presence, for the purpose of providing technical support, hardware and software maintenance, or assistance to UCPBS to troubleshoot, configure, update and check the performance of the Solution | |
| 2 | Technical Support and/or assistance shall include; the provision of analysis and recommendations and the performance or fulfillment of the recommendation/s. | |
| 3 | Technical Support Services shall be available from Mondays through Sundays, 24x7 (working-hours and non-working hours). | |
| 4 | <p><u>Location/s of Covered Components:</u></p> <ol style="list-style-type: none"> 1. 2nd floor, Overseas Filipino (OF) Bank Center Building, 1000 Liwasang Bonifacio, Intramuros, Barangay 656-A, 1000 Manila City, Philippines; 2. 2nd floor, UCPBS Disaster Recovery Site, 721 Aurora Blvd., Quezon City, Philippines | |
| 5 | <u>Scope of Local Support Services</u> | <u>Statement of Compliance</u> |
| | <p>a. The Supplier, through a Service or Help Desk, shall provide technical support assistance by electronic mail, telephone, and messaging platforms.</p>  | |

| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|----------------------|--|--|
| | | b. The Supplier's Service Desk shall be staffed with technically competent support engineers. The Service Desk shall be the single point-of-contact for UCPBS for Local Support Services. | |
| | | c. Service Desk operations shall be supported by the Supplier's internal electronic ticketing system, along with the necessary electronic mail and telephony systems. | |
| | | d. For support requests that cannot be resolved remotely, On-site support shall be provided by Supplier | |
| 6 | Support Level | <p>Supplier shall directly provide Levels 1 and 2 Technical Support to UCPBS's support requests. These Levels are defined as:</p> <ul style="list-style-type: none"> • Level 1 Technical Support – First-line support involving the tasks of problem identification, understanding UCPBS's expectations, initial problem diagnosis, and basic technical troubleshooting based on Supplier's knowledgebase of known problems and resolutions. • Level 2 Technical Support – Advanced Support involving the tasks of complex problem identification, in-depth problem diagnosis, and advanced technical troubleshooting. In some cases, if necessary, reproduction of the problem by Supplier, in coordination with UCPBS, is necessary to arrive at a solution. <p>Supplier shall facilitate resolution of support requests requiring Levels 3 and 4 support involving 3rd party supplier(s), including the Manufacturers-Principals, who developed and who have intellectual property rights over the Solution. These levels are defined as:</p> <ul style="list-style-type: none"> • Level 3 Technical Support – Support of this nature will require the involvement of the 3rd party supplier to conduct research and development to a new and/or unknown issue. Such issues shall require solutions such as bug fix, error correction, custom engineering or interim patch or fix for the Solution to operate as required by UCPBS, which only the 3rd Party supplier may provide. • Level 4 Technical Support – Support of this nature will involve the 3rd Party supplier's integration of the resolution to the Solution as an official patch, feature or capability. <p>Regardless of Support Level, UCPBS's concerns, incidents and queries may be referred to the 3rd Party supplier from whom the</p> | |

| Item # | TECHNICAL SPECIFICATIONS | | | | | | | | | | | | | | | | | | | | |
|----------------|--------------------------|--|----------------|--------------------|------------------------|---|---------|---------|---|---------|---------|---|---------|--------|---|---------|--------|---|-------|------|--|
| | | supported Solution originated without any additional cost to UCPBS. | | | | | | | | | | | | | | | | | | | |
| 7 | | <p>Service Management and Reporting</p> <ul style="list-style-type: none"> • Supplier shall handle and manage UCPBS's service requests in accordance with workflow procedures approved by UCPBS. • Quarterly reports on support requests and reported incidents will be completed by Supplier and submitted to UCPBS. • Quarterly status reports will be discussed by the Supplier Account Service Manager with UCPBS to ensure that UCPBS is aware of possible support issues and risks faced by UCPBS. | | | | | | | | | | | | | | | | | | | |
| 8 | | <p>Service Level Agreement</p> <table border="1"> <thead> <tr> <th>Severity Level</th> <th>Max. Response Time</th> <th>Max. Time Until Onsite</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>2 Hours</td> <td>4 Hours</td> </tr> <tr> <td>2</td> <td>3 Hours</td> <td>8 Hours</td> </tr> <tr> <td>3</td> <td>4 Hours</td> <td>2 Days</td> </tr> <tr> <td>4</td> <td>6 Hours</td> <td>4 Days</td> </tr> <tr> <td>5</td> <td>1 Day</td> <td>N.A.</td> </tr> </tbody> </table> <p>Severity Level 1</p> <ul style="list-style-type: none"> • Failure which causes major impact to UCPBS Business • Covered Solution or System is not operational. <p>Examples:</p> <ul style="list-style-type: none"> • System Hang (unable to save work in progress) • System functionality failure causes data losses or system unusable; • System down • Functionality failure renders system ineffective <p>Severity Level 2</p> <ul style="list-style-type: none"> • Failure causing severe degradation of UCPBS business • Covered Solution or System is not operating with full capability but is still operational. <p>Examples:</p> <ul style="list-style-type: none"> • Impaired or broken functionality with significant impact to applications; | Severity Level | Max. Response Time | Max. Time Until Onsite | 1 | 2 Hours | 4 Hours | 2 | 3 Hours | 8 Hours | 3 | 4 Hours | 2 Days | 4 | 6 Hours | 4 Days | 5 | 1 Day | N.A. | |
| Severity Level | Max. Response Time | Max. Time Until Onsite | | | | | | | | | | | | | | | | | | | |
| 1 | 2 Hours | 4 Hours | | | | | | | | | | | | | | | | | | | |
| 2 | 3 Hours | 8 Hours | | | | | | | | | | | | | | | | | | | |
| 3 | 4 Hours | 2 Days | | | | | | | | | | | | | | | | | | | |
| 4 | 6 Hours | 4 Days | | | | | | | | | | | | | | | | | | | |
| 5 | 1 Day | N.A. | | | | | | | | | | | | | | | | | | | |

| Item # | | TECHNICAL SPECIFICATIONS | | | | | | | | | | | | | | | |
|---|-------------------------|--|-------------------------------------|-------------------------|----------------------------|--|---|--|---------------------------------------|--|---|--|---|--|-------------------|--|--|
| | | <ul style="list-style-type: none"> • Frequent application failure, but no data loss; • Serious but predictable management system failure • Significant system performance degradation <p>Severity Level 3</p> <ul style="list-style-type: none"> • Degradation of machine performance causing inconvenience to the business. • Covered Solution or System is up and running with limited or no significant impacts. <p>Examples:</p> <ul style="list-style-type: none"> • Bugs which cause limited or no direct impact to performance and functionality • Request to replace a bug work-around; • Limited impact defective functionality • System performance support questions and issues <p>Severity Level 4</p> <ul style="list-style-type: none"> • A minor event causing little or no impact to UCPBS business. <p>Examples:</p> <ul style="list-style-type: none"> • Scheduled activities agreed with UCPBS • Methods of Procedure (MOP) <p>Severity Level 5</p> <ul style="list-style-type: none"> • The call is undergoing ongoing monitoring, but no further action is required. <p>Examples:</p> <ul style="list-style-type: none"> • Requests for status updates on action take'n/plans; Monitoring Reports/Feedback on action steps taken. | | | | | | | | | | | | | | | |
| 9 | | <p>System Requirements</p> <table border="1"> <thead> <tr> <th>Must support the following systems:</th> <th>Statement of Compliance</th> </tr> </thead> <tbody> <tr> <td>1. Operating System</td> <td></td> </tr> <tr> <td>• Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later</td> <td></td> </tr> <tr> <td>• Windows 8 Professional / Enterprise</td> <td></td> </tr> <tr> <td>• Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise</td> <td></td> </tr> <tr> <td>• Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise</td> <td></td> </tr> <tr> <td>2. Servers</td> <td></td> </tr> </tbody> </table> | Must support the following systems: | Statement of Compliance | 1. Operating System | | • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later | | • Windows 8 Professional / Enterprise | | • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise | | • Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise | | 2. Servers | | |
| Must support the following systems: | Statement of Compliance | | | | | | | | | | | | | | | | |
| 1. Operating System | | | | | | | | | | | | | | | | | |
| • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later | | | | | | | | | | | | | | | | | |
| • Windows 8 Professional / Enterprise | | | | | | | | | | | | | | | | | |
| • Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise | | | | | | | | | | | | | | | | | |
| • Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise | | | | | | | | | | | | | | | | | |
| 2. Servers | | | | | | | | | | | | | | | | | |

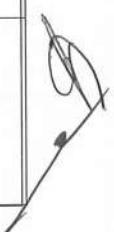


| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • Windows Small Business Server 2011 Essentials / Standard (64-bit) • Windows MultiPoint Server 2011 (64-bit); |
| | <ul style="list-style-type: none"> • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later • Windows Server 2012 Foundation / Essentials / Standard / Datacenter • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter • Windows Server 2016 Essentials / Standard / Datacenter; |
| | <ul style="list-style-type: none"> • Windows Server 2019 Essentials / Standard / Datacenter; |
| | <ul style="list-style-type: none"> • Windows Server 2022. |
| | <p>3. Microsoft Terminal Servers</p> <ul style="list-style-type: none"> • Microsoft Remote Desktop Services based on Windows Server 2008 R2 SP1 • Microsoft Remote Desktop Services based on Windows Server 2012 • Microsoft Remote Desktop Services based on Windows Server 2012 R2 • Microsoft Remote Desktop Services based on Windows Server 2016 • Microsoft Remote Desktop Services based on Windows Server 2019 • Microsoft Remote Desktop Services based on Windows Server 2022 |
| | <p>4. 32-bit Linux operating systems</p> <ul style="list-style-type: none"> • CentOS 6.7 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • Linux Mint 19 and later • Mageia 4 • Red Hat Enterprise Linux 6.7 and later • ALT Education 9 • ALT Workstation 9 |
| | <p>5. 64-bit Linux operating systems</p> |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <ul style="list-style-type: none"> • AlterOS 7.5 and later • Amazon Linux 2 • Astra Linux Common Edition (operational update 2.12). • Astra Linux Special Edition RUSB.10015-01 (operational update 1.5) • Astra Linux Special Edition RUSB.10015-01 (operational update 1.6) • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6) • CentOS 6.7 and later • CentOS 7.2 and later • CentOS 8.0 and later • Debian GNU / Linux 9.4 and later • Debian GNU / Linux 10.1 and later • EulerOS V2.0SP2 2.2.17 • EulerOS V2.0SP5 2.5.6 • Linux Mint 19 and later • Linux Mint 20.1 and later • openSUSE Leap 15.0 and later • Oracle Linux 7.3 and later • Oracle Linux 8.0 and later • Pardus OS 19.1 • Red Hat Enterprise Linux 6.7 and later • Red Hat Enterprise Linux 7.2 and later • Red Hat Enterprise Linux 8.0 and later • SUSE Linux Enterprise Server 12 SP5 and later • SUSE Linux Enterprise Server 15 and later • Ubuntu 18.04 LTS and later • Ubuntu 20.04 LTS • ALT Education 9 • ALT Workstation 9 • ALT Server 9 • GosLinux 7.2 • Red OS 7.3 <p>6. MAC OS operating systems:</p> <ul style="list-style-type: none"> • macOS 10.14 – 12 <p>7. The proposed solution must support the following virtual platforms:</p> <ul style="list-style-type: none"> • VMware Workstation 16.2.3; • VMware ESXi 7.0 Update 3d; • Microsoft Hyper-V Server 2019; | |

| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • Citrix Virtual Apps and Desktops 7 2203 LTSR; • Citrix Provisioning 2203 LTSR; • Citrix Hypervisor 8.2 LTSR (Cumulative Update 1). |
| | 8. The proposed solution must support protection of the latest Operating Systems versions across all platforms (Windows, Linux, MacOS, iOS, Android). |
| | 9. The proposed solution must be able to detect following types of threat: <ul style="list-style-type: none"> • Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software. |
| | 10. The proposed solution must support Anti-malware Scan Interface (AMSI). |
| | 11. The proposed solution must have the ability to integrate with Windows Defender Security Center. |
| | 12. The proposed solution must support Windows Linux subsystem. |
| | 13. The proposed solution must provide next gen protection technologies. For example: <ul style="list-style-type: none"> • protection against file-less threats • provision of multi-layered Machine Learning (ML) based protection and behavioral analysis during different stages of the kill-chain |
| | 14. The proposed solution must provide Memory Scanning for Windows workstations. |
| | 15. The proposed solution must provide Kernel Memory Scanning for Linux workstations. |
| | 16. The proposed solution must provide the ability to switch to cloud mode for threat protection, decreasing RAM and hard disk drive usage for resource-limited machines. |
| | 17. The proposed solution must have dedicated components to monitor, detect and block activities on Windows, Linux and Windows servers, and endpoints, to protect against remote encryption attacks. |
| | 18. The proposed solution must include signatureless components to detect threats even without frequent updates. Protection The proposed solution must be powered by Static ML for pre-execution and Dynamic ML for post-execution stages of the kill-chain on |



| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|--|---|--|
| | | endpoints and in the cloud for Windows servers and workstations. | |
| | | 19. The proposed solution must provide behavioral analysis based on ML. | |
| | | 20. The proposed solution must provide the ability to integrate with the vendor's own Endpoint Detection and Response (EDR) and Anti-APT solutions, for active threat hunting and automated incident response. | |
| | | 21. The proposed solution must support integration with a standalone/independent automated threat detection and prevention sandbox solution that does not depend on the vendor's EDR and /or Anti-APT solution. | |
| | | 22. The proposed solution must include the ability to configure and manage firewall settings built into the Windows Server and Linux operating systems, through its management console. | |
| | | 23. The proposed solution must include the following components in a single agent installed on the endpoint: <ul style="list-style-type: none"> • Application, Web and Device Controls • Anomaly Detection • HIPS and Firewall • Patch Management • Encryption | |
| | | 24. The proposed solution must provide Application and Device Controls for Windows workstations. | |
| | | 25. The proposed solution must include Application Launch/Start Control for the Windows Server operating system. | |
| | | 26. The proposed solution's protection for servers and workstations must include a dedicated component for protection against ransomware/cryptor virus activity on shared resources. | |
| | | 27. The proposed solution must, on detecting ransomware/cryptor-like activity, automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type. | |
| | | 28. The proposed solution must provide a pre-defined list of scan exclusions for Microsoft applications and services. | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <p>29. The proposed solution should support the installation of endpoint protection on servers without the need to restart.</p> <p>30. The proposed solution must enable the following for endpoints:</p> <ul style="list-style-type: none"> • Manual Scanning • On-Access Scanning • On-Demand Scanning • Compressed File Scanning • Scan Individual File, Folder and Drive • Script Blocking and Scanning • Registry Guard • Buffer Overflow Protection • Background/Idle Scanning • Removable Drive Scanning on connection with system • The ability to detect and block untrusted hosts on detection of encryption-like activities on server shared resources. | |
| | <p>31. The proposed solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.</p> | |
| | <p>32. The proposed solution must have both local and global reputation databases.</p> | |
| | <p>33. The proposed solution must be able to scan HTTPS, HTTP and FTP traffic against viruses and spyware, or any other malware.</p> | |
| | <p>34. The proposed solution must include a personal firewall capable, as an absolute minimum, of:</p> <ul style="list-style-type: none"> • Blocking network activates of applications based on their categorization. • Blocking/allowing specific packets, protocols, IP addresses, ports and traffic direction. • The automatic and manual addition of network subnets, and modification of network activity permissions. | |
| | <p>35. The proposed solution must prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization.</p> | |
| | <p>36. The proposed solution must be able to block network attacks and report the source of the infection.</p> | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <p>37. The proposed solution must have local storage on endpoints to keep copies of files that have been deleted or modified during disinfection. These files must be stored in a specific format that ensures they cannot pose any threat.</p> | |
| | <p>38. The proposed solution must have a proactive approach to preventing malware from exploiting existing vulnerabilities on servers and workstations.</p> | |
| | <p>39. The proposed solution must support AM-PPL (Anti-Malware Protected Process Light) technology for protection against malicious actions.</p> | |
| | <p>40. The proposed solution must include protection against attacks that exploit vulnerabilities in the ARP protocol in order to spoof the device MAC address.</p> | |
| | <p>41. The proposed solution must include a control component able to learn to recognize typical user behavior in a specific individual or group of protected computers, then identify and block anomalous and potentially harmful actions made by that endpoint or user.</p> | |
| | <p>42. The proposed solution must provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections.</p> | |
| | <p>43. The proposed solution must include a dedicated component for scanning encrypted connections.</p> | |
| | <p>44. The proposed solution must be able to decrypt and scan network traffic transmitted over encrypted connections supported by the following protocols; SSL 3.0, TLS 1.0, TLS1.1, TLS1.2, TLS 1.3.</p> | |
| | <p>45. The proposed solution must have the ability to automatically exclude web resources when a scan error occurs while performing an encrypted.</p> | |
| | <p>46. The proposed solution must include functionality to remotely wipe data on the endpoint (for workstations).</p> | |
| | <p>47. The proposed solution must have following remote data wipe functionalities:</p> <ul style="list-style-type: none"> • In silent mode • On hard drives and removable drives • For all user accounts on the computer | |
| | <p>48. The proposed solution's remote data wipe functionality must support the following modes:</p> | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| | <ul style="list-style-type: none"> • Immediate data deletion • Postponed data deletion |
| | <p>49. The proposed solution's remote data wipe functionality must support the following data deletion methods:</p> <ul style="list-style-type: none"> • Delete by using the operating resources - files are deleted but are not sent to the recycle bin • Delete completely, without recovery - making data practically impossible to restore after deletion. |
| | <p>50. The proposed solution must include functionality to automatically delete the data if there is no connection to the endpoint management server.</p> |
| | <p>51. The proposed solution must support signature-based detection in addition to cloud-assisted and heuristics.</p> |
| | <p>52. The proposed solution should have the ability to raise an alert on, clean, and delete a detected threat.</p> |
| | <p>53. The proposed solution should have the ability to accelerate scanning tasks, skipping those objects that have not changed since the previous scan.</p> |
| | <p>54. The proposed solution should have the ability to prioritize custom and on-demand scanning tasks for Linux workstations.</p> |
| | <p>55. The proposed solution must allow the administrator to exclude specified files/ folders/applications/digital certificates from being scanned, either on-access (real-time protection) or during on-demand scans.</p> |
| | <p>56. The proposed solution should include the functionality to isolate infected computers.</p> |
| | <p>57. The proposed solution must automatically scan removable drives for malware when they are attached to any endpoint. Scan control should be based on drive size.</p> |
| | <p>58. The proposed solution must be able to block the use of USB storage devices or allow access only to permitted devices, and allow read/write access only by domain users, to reduce data theft and enforce lock policies.</p> |
| | <p>59. The proposed solution must be able to differentiate between USB storage devices, printers, mobiles and other peripherals.</p> |
| | <p>60. The proposed solution must be able to log file operations (Write and Delete) on USB storage devices. This should not require any additional license or component to be installed on the endpoint.</p> |



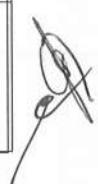
| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <p>61. The proposed solution must have ability to block the execution of any executable from the USB storage device.</p> | |
| | <p>62. The proposed solution must have ability to block/allow user access to web resources based on websites, content type, user and time of day.</p> | |
| | <p>63. The proposed solution must have a specific detection category to block website banners.</p> | |
| | <p>64. The proposed solution must provide the ability to configure Wi-Fi networks based on Network Name, Authentication Type, Encryption Type, so these can later be used to block or allow the Wi-Fi connections.</p> | |
| | <p>65. The proposed solution must support user-based policies for Device, Web and Application Control.</p> | |
| | <p>66. The proposed solution should specifically allow the blocking of the following devices:</p> <ul style="list-style-type: none"> • Bluetooth • Mobile devices • External modems • CD/DVDs • Cameras and Scanners • MTPs • And the transfer of data to mobile devices | |
| | <p>67. The proposed solution should feature cloud integration, to provide the fastest possible updates on malware and potential threats.</p> | |
| | <p>68. The proposed solution must have ability to manage user access rights for Read and Write operations on CDs/DVDs, removable storage devices and MTP devices.</p> | |
| | <p>69. The proposed solution must feature firewall filtering by local address, physical interface, and packet Time-To-Live (TTL).</p> | |
| | <p>70. The proposed solution must allow the administrator to monitor the application's use of custom/random ports after it has launched.</p> | |
| | <p>71. The proposed solution must support the blocking of prohibited (Deny-List) applications from being launched on the endpoint, and the blocking of all applications other than those included in Allow-Lists.</p> | |
| | <p>72. The proposed solution must have a cloud-integrated Application Control component for immediate access to the latest updates on application ratings and categories.</p> | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | 73. The proposed solution must offer protection to files executed in Windows Server containers. | |
| | 74. The proposed solution must include traffic malware filtering, web link verification and web-resource control based on cloud categories. | |
| | 75. The proposed solution Web Control/Restriction component must include a Cryptocurrencies and Mining category. It must also include predefined regional legal restrictions to comply with Belgian and Japanese Law. | |
| | 76. The proposed solution must have the ability to allow applications based on their digital signature certificates, MD5, SHA256, META Data, File Path, and pre-defined security categories. | |
| | 77. The proposed solution must have controls for the download of DLL and Drivers. | |
| | 78. The proposed solution's application control component must include Deny List and Allow List operational modes. | |
| | 79. The proposed solution must support the control of scripts from PowerShell. | |
| | 80. The proposed solution must support Test Mode with report generation on the launch of blocked applications. | |
| | 81. The proposed solution must have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files "HIPS functionality". | |
| | 82. The proposed solution must have the ability to control system/user application access to audio and video recording devices. | |
| | 83. The proposed solution must provide a facility to check applications listed in each cloud-based category. | |
| | 84. The proposed solution must have ability to integrate with a vendor-specific Advanced Threat Protection system. | |
| | 85. The proposed solution must have ability to automatically regulate the activity of programs running, including access to the file system and registry as well as interaction with other programs. | |
| | 86. The proposed solution must have the ability to automatically delete Application Control rules if an | |

| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|-----|---|--|
| | | application is not launched during a specified interval. The interval must be configurable. | |
| | 87. | The proposed solution must have ability to automatically categorize applications launched prior to endpoint protection installation. | |
| | 88. | The proposed solution must have endpoint mail threat protection with: <ul style="list-style-type: none"> • Attachment filter and the ability to rename attachments. • Scanning of mail messages when receiving, reading and sending. | |
| | 89. | The proposed solution must have the ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays. | |
| | 90. | The proposed solution must enable the user of the computer to perform a check on a file's reputation from the File Context menu. | |
| | 91. | The proposed solution must include the scanning of all scripts, including those developed in Microsoft Internet Explorer, as well as any WSH scripts (JavaScript, Visual Basic Script WSH scripts (JavaScript, Visual Basic Script etc.), launched when the user works on the computer, including the internet. | |
| | 92. | The proposed solution must provide protection against as yet unknown malware based of the analysis of their behavior and examination of changes in the system register, together with a strong remediation engine to automatically restore any system changes made by the malware. | |
| | 93. | The proposed solution must provide protection against hacker attacks by using a firewall with an intrusion detection and prevention system (IDS/IPS) and network activity rules for more popular applications when working in computer networks of any type, including wireless networks. | |
| | 94. | The proposed solution must include IPv6 protocol support. | |
| | 95. | The proposed solution must offer scanning of critical sections of the computer as a standalone task. | |
| | 96. | The proposed solution must incorporate Application Self-Protection technology: <ul style="list-style-type: none"> • protecting against unauthorized the remote management of an application service. | |

| TECHNICAL SPECIFICATIONS | | | | | | |
|---|--|--------------------------------|--|---|---|--|
| Item # | | | | | | |
| | <ul style="list-style-type: none"> • protecting access to application parameters by setting a password. • preventing the disabling of protection by malware, criminals or amateur users. | | | | | |
| | 97. The proposed solution must offer the ability to choose which threat protection components to install. | | | | | |
| | 98. The proposed solution must include the antivirus checking and disinfection of files that have been packed using programs like PKLITE, LZEXE, DIET, EXEPACK, etc. | | | | | |
| | 99. The proposed solution must include the anti-malware checking and disinfection of files in archives using the RAR, ARJ, ZIP, CAB, LHA, JAR, ICE formats, including password-protected files. | | | | | |
| | 100. The proposed solution must protect against as yet unknown malware belonging to registered families, based on heuristic analysis. | | | | | |
| | 101. The proposed solution must include multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry). | | | | | |
| | 102. The proposed solution must allow the administrator to create a single installer with the required configuration, for use by non-IT literate users. | | | | | |
| | Mobile Device Management <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left; padding-bottom: 5px;">Statement of Compliance</th></tr> <tr> <td>1. The proposed solution should be able to protect or manage Android mobile devices: <ul style="list-style-type: none"> • Android 5-13 (excluding Go edition) </td></tr> <tr> <td>2. The proposed solution should be able to protect or manage iOS mobile devices: <p>iOS mobile device management:</p> <ul style="list-style-type: none"> • iOS 10.0–15.0 or iPadOS 13–15 <p>iOS online protection:</p> <ul style="list-style-type: none"> • iOS 14.1 or later • iPadOS 14.1 or later </td></tr> <tr> <td>3. The proposed solution must support Huawei Mobile Services.</td></tr> <tr> <td>4. The proposed solution must enable protection of the smartphone file system and the interception and scanning of all incoming objects transferred through wireless connections (infrared port, Bluetooth), EMS</td></tr> </table> | Statement of Compliance | 1. The proposed solution should be able to protect or manage Android mobile devices: <ul style="list-style-type: none"> • Android 5-13 (excluding Go edition) | 2. The proposed solution should be able to protect or manage iOS mobile devices: <p>iOS mobile device management:</p> <ul style="list-style-type: none"> • iOS 10.0–15.0 or iPadOS 13–15 <p>iOS online protection:</p> <ul style="list-style-type: none"> • iOS 14.1 or later • iPadOS 14.1 or later | 3. The proposed solution must support Huawei Mobile Services. | 4. The proposed solution must enable protection of the smartphone file system and the interception and scanning of all incoming objects transferred through wireless connections (infrared port, Bluetooth), EMS |
| Statement of Compliance | | | | | | |
| 1. The proposed solution should be able to protect or manage Android mobile devices: <ul style="list-style-type: none"> • Android 5-13 (excluding Go edition) | | | | | | |
| 2. The proposed solution should be able to protect or manage iOS mobile devices: <p>iOS mobile device management:</p> <ul style="list-style-type: none"> • iOS 10.0–15.0 or iPadOS 13–15 <p>iOS online protection:</p> <ul style="list-style-type: none"> • iOS 14.1 or later • iPadOS 14.1 or later | | | | | | |
| 3. The proposed solution must support Huawei Mobile Services. | | | | | | |
| 4. The proposed solution must enable protection of the smartphone file system and the interception and scanning of all incoming objects transferred through wireless connections (infrared port, Bluetooth), EMS | | | | | | |



| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|-----|---|--|
| | | and MMS, while synchronizing with the personal computer and uploading files through a browser. | |
| | 5. | The proposed solution must have the ability to block malicious sites designed to spread malicious code, and phishing websites designed to steal confidential user data and access the user's financial information. | |
| | 6. | The proposed solution must have the functionality to add a website excluded from the scan to an Allow List. | |
| | 7. | The proposed solution must include website filtering by categories and allow the administrator to restrict user access to specific categories (for example, gambling-related websites or social media categories). | |
| | 8. | The proposed solution must enable the administrator to obtain information about the operation of antivirus and web protection on the user's mobile device. | |
| | 9. | The proposed solution must have the functionality to detect the location of the mobile device location via GPS, and show this on Google Maps. | |
| | 10. | The proposed solution must enable the administrator to take a picture (Mugshot) from the front camera of the mobile when it's locked. | |
| | 11. | The proposed solution must have containerization capabilities for Android devices. | |
| | 12. | The proposed solution must have the functionality to remotely wipe the following from Android devices: <ul style="list-style-type: none"> • containerized data • corporate email accounts | |
| | 13. | The proposed solution must have the functionality to remotely wipe the following from iOS devices: <ul style="list-style-type: none"> • All installed configuration profiles • All provisioning profiles • The iOS MDM profile • Applications for which Remove and the iOS MDM profile check box have been selected | |
| | 14. | The proposed solution must allow the encryption of all data on the device (including user account data, removable drives and apps, as well as email messages, SMS messages, contacts, photos, and other files). Access to encrypted data should only be possible on an unlocked device through a special key or device unlock password. | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <p>15. The proposed solution must offer controls to ensure that all devices comply with corporate security requirements. Compliance Control should be based on a set of rules which should include the following components:</p> <ul style="list-style-type: none"> • Device check criteria • Time period allocated for the user to fix the non-compliance • action that will be taken on the device if the user does not fix the non-compliance within the set time period • Ability to remediate non-compliant devices | |
| | <p>16. The proposed solution must have the functionality to detect and to notify the administrator about device hacks (e.g. rooting/jailbreak).</p> | |
| | <p>17. The proposed solution should enable management of the following device features:</p> <ul style="list-style-type: none"> • Memory cards and other removable drives • Device camera • Wi-Fi connections • Bluetooth connections • Infrared connection port • Wi-Fi access point activation • Remote desktop connection • Desktop synchronization • Configure Exchange Mailbox settings • Configure mailbox on iOS MDM devices • Configure Samsung KNOX containers. • Configure the settings of the Android for Work profile • Configure Email/Calendar/Contacts • Configure Media content restriction settings. • Configure proxy settings on the mobile device • Configure certificates and SCEP | |
| | <p>18. The proposed solution should allow the configuration of a connection to AirPlay devices to enable the streaming of music, photos, and videos from the iOS MDM device to AirPlay devices.</p> | |
| | <p>19. The proposed solution must support all the below deployment methods for the mobile agent:</p> <ul style="list-style-type: none"> • Google Play, Huawei App Gallery and Apple App Store <ul style="list-style-type: none"> • KNOX Mobile Enrollment portal • Standalone preconfigured installation packages | |



| TECHNICAL SPECIFICATIONS | |
|--------------------------|---|
| Item # | |
| | 20. The proposed solution must allow the configuration of Access Point Names (APN) to connect a mobile device to data transfer services on a mobile network. |
| | 21. The proposed solution must allow the PIN on a mobile device to be reset remotely. |
| | 22. The proposed solution must include the option to enroll Android devices using 3rd party EMM systems: <ul style="list-style-type: none">• VMware AirWatch 9.3 or later• MobileIron 10.0 or later• IBM MaaS360 10.68 or later• Microsoft Intune 1908 or later<ul style="list-style-type: none">• SOTI MobiControl 14.1.4 (1693) or later |
| | 23. The proposed solution must have the functionality to enforce the installation of a mandatory app on the device. |
| | 24. The proposed solution must support user-initiated mobile agent deployment via: <ul style="list-style-type: none">• Google Play• Huawei App Gallery• Apple App Store |
| | 25. The proposed solution must be able to scan files opened on the device. |
| | 26. The proposed solution must be able to scan programs installed from the device interface. |
| | 27. The proposed solution must be able to scan file system objects on the device or on connected memory extension cards on request of the user or according to a schedule. |
| | 28. The proposed solution must provide the reliable isolation of infected objects in a quarantine storage location. |
| | 29. The proposed solution must feature the updating of antivirus databases used to search for malicious programs and deleting dangerous objects. |
| | 30. The proposed solution must be able to scan mobile devices for malware and other unwanted objects on-demand and on-schedule and deal with them automatically. |
| | 31. The proposed solution must be able to manage and monitor mobile devices from same console as that used to manage computers and servers. |



| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|--|---|--------------------------------|
| | | 32. The proposed solution must provide Anti-Theft functionality, so that lost and/or displaced devices can be located, locked and wiped remotely. | |
| | | 33. The proposed solution must provide the facility to block forbidden applications from being launched on the mobile device. | |
| | | 34. The proposed solution must be able to remotely install and remove applications from iOS devices. | |
| | | 35. The proposed solution must be able to enforce security settings, such as password restrictions and encryption, on mobile devices. | |
| | | 36. The proposed solution must have the ability to push applications recommended/required by the administrator to the mobile phone. | |
| | | 37. The proposed solution must include a subscription model. | |
| | | 38. The proposed solution must protect from online threats on iOS devices. | |
| | | Encryption | Statement of Compliance |
| | | <p>1. The proposed solution must support encryption on multiple levels:</p> <ul style="list-style-type: none"> • Full disk encryption – including system disk • File and folder encryption • Removable media encryption <p>BitLocker and MacOS Filevault2 Encryption Management</p> | |
| | | <p>2. The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows:</p> <ul style="list-style-type: none"> • The encryption of files on local computer drives. • The creation of encryption lists of files by extension or group of extensions. <p>The creation of encryption lists of folders on local computer drives.</p> | |
| | | <p>3. The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows the encryption of files on removable drives. This must include the ability to:</p> <ul style="list-style-type: none"> • Specify a default encryption rule by which the application applies the same action to all removable drives. | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <p>Configure encryption rules for files stored on individual removable drives.</p> <p>4. The proposed solution must offer integrated File Level Encryption (FLE) functionality that supports several file encryption modes for removable drives:</p> <ul style="list-style-type: none"> • The encryption of all files stored on removable drives <p>The encryption of new files only as they are saved or created on removable drives.</p> <p>5. The proposed solution must offer Integrated File Level Encryption (FLE) functionality that allows files on removable drives be encrypted in portable mode. It must allow access to encrypted files on removable drives that are connected to computers without encryption functionality.</p> <p>6. The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows the encryption of all files that specific applications can create or modify, on both hard drives and removable drives.</p> <p>7. The proposed solution must offer integrated File Level Encryption (FLE) functionality that enables the management of rules of application access to encrypted files, including defining of an encrypted file access rule for any application. It must enable the blocking of access to encrypted files, or the allowing of access to encrypted files as ciphertext only.</p> <p>8. The proposed solution must offer the capability to restore encrypted devices if an encrypted hard drive or removable drive is corrupted.</p> <p>9. The proposed solution must offer Integrated Full Disk Encryption (FDE) functionality for hard drives and removable drives. As with FLE, there must be the capability to specify a default encryption rule by which the application applies the same action to all removable drives, or to configure encryption rules for individual removable drives.</p> <p>10. The proposed solution must offer an encryption module which is managed centrally on all computers, with ability to enforce encryption policies and modify/stop encryption settings.</p> | |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | 11. The proposed solution must offer the ability to centrally monitor encryption status and to generate reports regarding encrypted computers/devices. | |
| | 12. The proposed solution must offer encryption that is fully transparent to end users and has no adverse impact on system performance and usage. | |
| | 13. The proposed solution must offer Full Disk Encryption that supports the central management of authorized users, including adding, removing and password reset. Only authorized users should have permission to boot the encrypted disk. | |
| | 14. The proposed solution must have the facility to block application access to encrypted data if needed. | |
| | 15. The proposed solution must support the automatic encryption of removable storage devices and must be able to prevent data being copied to unencrypted media. | |
| | 16. The proposed solution must provide a facility for creating password-protected containers which can be used to exchange data with external users. | |
| | 17. The proposed solution must provide a central location for encryption key storage, and multiple recovery options. | |
| | 18. The proposed solution's administrator/management server must have the ability to decrypt all encrypted data. regardless of location and/or user. | |
| | 19. The proposed solution must support both QWERTY and AZERTY keyboard layouts for pre-boot authorization. | |
| | 20. The proposed solution must support pre-boot authorization for following devices: Safe Net eToken 4100, Gemalto IDPrime .NET (511), Rutooken ECP Flash. | |
| | 21. The proposed solution must provide the functionality to manage/apply Microsoft Bit locker encryption. | |
| | 22. The proposed solution must provide the functionality to customize Microsoft BitLocker encryption settings including: <ul style="list-style-type: none"> • Use of Trusted Platform Module and password settings. • Use of hardware encryption for workstations and software encryption if Hardware encryption not available. | |

| TECHNICAL SPECIFICATIONS | |
|--------------------------|--|
| | <p>Use of authentication requiring data input in a preboot environment, even if the platform does not have the capability for preboot input (for example, with touchscreen keyboards on tablets).</p> <p>23. The proposed solution must support Encryption on Microsoft Surface Tablets.</p> |
| | <p>Systems Management, vulnerability and patch management</p> <p>1. The proposed solution should include features to manage computers remotely, including:</p> <ul style="list-style-type: none"> • Remote installation of third-party software • Reporting on existing software and hardware • Monitoring for the installation of unauthorized software <p>Removal of unauthorized software</p> <p>2. The proposed solution should include patch management capabilities for Windows operating systems and for installed third-party applications.</p> <p>3. The proposed solution's patch management functionality should be fully automated, with ability to detect, download and push missing patches to endpoints.</p> <p>4. The proposed solution must provide the facility to select which patches are to be downloaded/pushed to endpoints, based on their criticality.</p> <p>5. The proposed solution must be able to detect existing vulnerabilities in operating systems and other installed applications, and then to respond by automatically downloading/pushing the necessary patches to endpoints.</p> <p>6. The proposed solution must provide comprehensive reports on discovered vulnerabilities and missing patches, as well as on endpoints and patch deployment status.</p> <p>7. The proposed solution should have the capability to push specific patches based on criticality or severity.</p> <p>8. The proposed solution management server must be configurable as an updates source for Microsoft Updates and third-party applications.</p> <p>9. The proposed solution must include the vulnerability advisory of application vendor as well as security vendor.</p> |
| | <p>Statement of Compliance</p> |

| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| | <p>10. The proposed solution must enable the administrator to approve updates.</p> <p>11. The proposed solution must be able to automatically identify missing patches on individual endpoints and push only which are needed/missing.</p> <p>12. The proposed solution should support patch aggregation to minimize number of updates needed.</p> <p>13. The proposed solution should notify the administrator of any patches missing from endpoints as soon as the relevant information is available.</p> <p>14. The proposed solution should provide the facility to manage patching separately for operating systems and for third-party applications.</p> <p>15. The proposed solution should provide the facility to fix existing vulnerabilities either on any endpoint or only on specific ones.</p> <p>16. The proposed solution should provide the facility to automatically detect/install all previously missed patches which are required to apply selected patch (dependencies).</p> <p>17. The proposed solution must support the automated distribution of patches and updates for 150+ applications.</p> <p>18. The proposed solution must have patch testing mode support functionality,</p> <p>19. The proposed solution must include dedicated fields that contain information about ‘Exploit found for the vulnerability’.</p> <p>20. The proposed solution must include dedicated fields that contain information about ‘Threat found for the vulnerability’.</p> <p>21. The proposed solution must allow the administrator to restrict device users’ ability to apply Microsoft Updates themselves.</p> <p>22. The proposed solution must allow the administrator to specify which updates can be installed by users.</p> <p>23. The proposed solution must enable the administrator to view a list of updates and patches unrelated to client devices.</p> <p>24. The proposed solution must support operating system deployment.</p> <p>25. The proposed solution must support Wake-on LAN and UEFI.</p> |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | 26. The proposed solution must have built-in remote desktop sharing functionality. All file operations performed on the remote endpoint during the session must be logged on the Management Server. |
| | 27. The proposed solution must be able to deliver vulnerability fixes to client computers without installing the updates. |
| | 28. The proposed solution must allow the administrator to choose Windows updates to install, after which the client device user can install only those updates allowed/selected by the administrator. |
| | 29. The proposed solution must inform the administrator about unrelated updates and patches on the client device. |
| | 30. The proposed solution must be configurable/assignable as an update source for Microsoft and third-party updates. |
| | 31. The proposed solution must allow the administrator to select the Microsoft product and languages for which updates are downloaded. |
| | 32. The proposed solution must be able to remotely push/deploy EXE, MSI, bat, cmd, MSP files, and allow the administrator to define the command line parameter for the remote installation. |
| | 33. The proposed solution must be able to remotely uninstall applications, not limited to incompatible Anti-Virus programs. |
| | 34. The proposed solution must allow the administrator to use single task/job and to define different vulnerability-fix rules or criteria for Microsoft and third-party applications updates. |
| | 35. The proposed solution must allow the administrator set up rules for Microsoft and Third-party patch/update installation: <ul style="list-style-type: none"> • Start installation at computer restart or shutdown. • Install the required general system prerequisites. • Allow the installation of new application versions during updates. |
| | Download updates to the device without installing them. |
| | 36. The proposed solution must have ability to test the installation of updates on a percentage of computers before application to all target computers. The administrator must be able to configure the number of |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--------------------------------|
| | test computers as a percentage, and the time allocated prior to full rollout in terms of hours. | |
| | 37. The proposed solution must enable the removal/uninstallation of specified application and operating system updates. | |
| | 38. The proposed solution management server must be able to send logs to SIEMs and SYSLOG servers. | |
| | 39. The proposed solution must be able to track third party application licenses and raise notifications of any potential violations. | |
| | 40. The proposed solution's reporting must contain CVE information. | |
| | Centralized administration, monitoring, and update software requirements | Statement of Compliance |
| | <p>1. The proposed solution must support installation on the following Operating Systems:</p> <p>Windows:</p> <ul style="list-style-type: none"> • Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit • Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit • Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit • Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit • Microsoft Windows 10 Pro 19H1 32-bit/64-bit • Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit • Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit • Microsoft Windows 10 Education 19H1 32-bit/64-bit • Microsoft Windows 10 Pro 19H2 32-bit/64-bit • Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit • Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit • Microsoft Windows 10 Education 19H2 32-bit/64-bit • Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-bit/64-bit | |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <ul style="list-style-type: none"> • Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-bit/64-bit • Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-bit/64-bit <p>Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-bit/64-bit</p> <ul style="list-style-type: none"> • Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-bit/64-bit • Microsoft Windows 11 Home 64-bit • Microsoft Windows 11 Pro 64-bit • Microsoft Windows 11 Enterprise 64-bit • Microsoft Windows 11 Education 64-bit • Microsoft Windows 8.1 Pro 32-bit/64-bit • Microsoft Windows 8.1 Enterprise 32-bit/64-bit • Microsoft Windows 8 Pro 32-bit/64-bit • Microsoft Windows 8 Enterprise 32-bit/64-bit • Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit • Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit | |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <ul style="list-style-type: none"> • Windows Server 2008 R2 Standard with Service Pack 1 and higher 64-bit • Windows Server 2008 R2 with Service Pack 1 (all editions) 64-bit • Windows Server 2012 Server Core 64-bit • Windows Server 2012 Datacenter 64-bit • Windows Server 2012 Essentials 64-bit • Windows Server 2012 Foundation 64-bit • Windows Server 2012 Standard 64-bit • Windows Server 2012 R2 Server Core 64-bit • Windows Server 2012 R2 Datacenter 64-bit • Windows Server 2012 R2 Essentials 64-bit • Windows Server 2012 R2 Foundation 64-bit • Windows Server 2012 R2 Standard 64-bit • Windows Server 2016 Datacenter (LTSB) 64-bit Windows Server 2016 Standard (LTSB) 64-bit <ul style="list-style-type: none"> • Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit • Windows Server 2019 Standard 64-bit • Windows Server 2019 Datacenter 64-bit • Windows Server 2019 Core 64-bit • Windows Server 2022 Standard 64-bit • Windows Server 2022 Datacenter 64-bit • Windows Server 2022 Core 64-bit • Windows Storage Server 2012 64-bit • Windows Storage Server 2012 R2 64-bit • Windows Storage Server 2016 64-bit • Windows Storage Server 2019 64-bit Linux: <ul style="list-style-type: none"> • Debian GNU/Linux 11.x (Bullseye) 32-bit/64-bit • Debian GNU/Linux 10.x (Buster) 32-bit/64-bit • Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit • Ubuntu Server 20.04 LTS (Focal Fossa) 64-bit • Ubuntu Server 18.04 LTS (Bionic Beaver) 64-bit • CentOS 7.x 64-bit • Red Hat Enterprise Linux Server 8.x 64-bit • Red Hat Enterprise Linux Server 7.x 64-bit • SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit • SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit | |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | <ul style="list-style-type: none"> • Astra Linux Special Edition 1.7 (including the closed software environment mode and the mandatory mode) 64-bit • Astra Linux Special Edition 1.6 (including the closed software environment mode and the mandatory mode) 64-bit • Astra Linux Common Edition 2.12 64-bit • Alt Server 10 64-bit • Alt Server 9.2 64-bit • Alt 8 SP Server (LKNV.11100-01) 64-bit • Alt 8 SP Server (LKNV.11100-02) 64-bit • Alt 8 SP Server (LKNV.11100-03) 64-bit • Oracle Linux 7 64-bit • Oracle Linux 8 64-bit • RED OS 7.3 Server 64-bit • RED OS 7.3 Certified Edition 64-bit <p>2. The proposed solution must support the following database servers:</p> <ul style="list-style-type: none"> • Microsoft SQL Server 2012 Express 64-bit • Microsoft SQL Server 2014 Express 64-bit • Microsoft SQL Server 2016 Express 64-bit • Microsoft SQL Server 2017 Express 64-bit • Microsoft SQL Server 2019 Express 64-bit • Microsoft SQL Server 2014 (all editions) 64-bit • Microsoft SQL Server 2016 (all editions) 64-bit • Microsoft SQL Server 2017 (all editions) on Windows 64-bit • Microsoft SQL Server 2017 (all editions) on Linux 64-bit <ul style="list-style-type: none"> • Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions) • Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions) • Microsoft Azure SQL Database • All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms • MySQL 5.7 Community 32-bit/64-bit • MySQL Standard Edition 8.0 (release 8.0.20 and higher) 32-bit/64-bit • MySQL Enterprise Edition 8.0 (release 8.0.20 and higher) 32-bit/64-bit • MariaDB 10.5.x 32-bit/64-bit • MariaDB 10.4.x 32-bit/64-bit • MariaDB 10.3.22 and higher 32-bit/64-bit | |

| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <ul style="list-style-type: none"> • MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine • MariaDB Galera Cluster 10.3 32-bit/64-bit with InnoDB storage engine • MariaDB 10.1.30 and higher 32-bit/64-bit |
| | <p>3. The proposed solution must support the following virtual platforms:</p> <ul style="list-style-type: none"> • VMware vSphere 6.7 • VMware vSphere 7.0 • VMware Workstation 16 Pro • Microsoft Hyper-V Server 2012 64-bit • Microsoft Hyper-V Server 2012 R2 64-bit • Microsoft Hyper-V Server 2016 64-bit • Microsoft Hyper-V Server 2019 64-bit • Microsoft Hyper-V Server 2022 64-bit • Citrix XenServer 7.1 LTSR • Citrix XenServer 8.x • Parallels Desktop 17 • Oracle VM VirtualBox 6.x (Windows guest login only) |
| | <p>4. The proposed solution must enable the installation of anti-malware software from a single distribution package.</p> |
| | <p>5. The proposed solution must have customizable installation profiles depending on the number of protected nodes.</p> |
| | <p>6. The proposed solution must support IPv6 addresses.</p> |
| | <p>7. The proposed solution must support two-step verification (authentication).</p> |
| | <p>8. The proposed solution must have ability to read information from Active Directory to obtain data about computer accounts in the organization.</p> |
| | <p>9. The proposed solution must include a built-in web console for the management of the endpoints, which should not require any additional installation.</p> |
| | <p>10. The proposed solution's web management console should be straightforward to use and must support touch screen devices.</p> |
| | <p>11. The proposed solution must automatically distribute computer accounts by management group if new computers appear on the network. It must provide the ability to set the transfer rules according IP address,</p> |

| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|--|--|--|
| | | <p>type of the operating system and location in Organizational Units of Active Directory.</p> <p>12. The proposed solution must provide for the centralized installation, update and removal of anti-malware software, together with centralized configuration, administration, and the viewing of reports and statistical information about its operation.</p> <p>13. The proposed solution must feature the centralized removal (manual and automatic) of incompatible applications from the administration center.</p> <p>14. The proposed solution must provide flexible methods for anti-malware agent installation: RPC, GPO, an administration agent for remote installation and the option to create a standalone installation package for local installation.</p> <p>15. The proposed solution must enable the remote installation of anti-malware software with the latest anti-malware databases.</p> <p>16. The proposed solution must enable the automatic update of anti-malware software and anti-malware databases.</p> <p>17. The proposed solution must have automatic search facilities for vulnerabilities in applications and in the operating system on protected machines.</p> <p>18. The proposed solution must enable the management of a component prohibiting the installation and/or running of programs.</p> <p>19. The proposed solution must enable the management of a component controlling work with external I/O devices.</p> <p>20. The proposed solution must enable the management of a component controlling user activity on the internet.</p> <p>21. The proposed solution must allow for the testing of downloaded updates by means of the centralized administration software prior to distributing them to client machines, and the delivery of updates to user workplaces immediately after receiving them.</p> <p>22. The proposed solution must be able to automatically deploy protection to virtual infrastructures based on VMware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization platform or hypervisor.</p> <p>23. The proposed solution must enable the creation of a hierarchy of administration servers at an arbitrary</p> | |

| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|-----|--|--|
| | | level and the ability to centrally managing the entire hierarchy from the upper level. | |
| | 24. | The proposed solution must support Managed Services Mode for administration servers, so that logically isolated administration server instances can be set up for different users and user groups. | |
| | 25. | The proposed solution must give access to the anti-malware security vendor's cloud services via the administration server. | |
| | 26. | The proposed solution must include the automatic distribution of licenses on client computers. | |
| | 27. | The proposed solution must be able to perform inventories of software and hardware installed on user computers. | |
| | 28. | The proposed solution must have a notification mechanism to inform users about events in the installed anti-malware software and settings, and to distribute notifications about events via email. | |
| | 29. | The proposed solution must enable the centralized installation of third-party applications on all or selected computers. | |
| | 30. | The proposed solution must have the ability to specify any computer in the organization as a center for relaying updates and installation packages, in order to reduce the network load on the main administration server system. | |
| | 31. | The proposed solution must have the ability to specify any computer in the organization as a center for forwarding anti-malware agent events from the selected group of client computers to the centralized administration server, in order to reduce the network load on the main administration server system. | |
| | 32. | The proposed solution must be able to generate graphical reports for anti-malware software events, and data about the hardware and software inventory, licensing, etc. | |
| | 33. | The proposed solution must be able to export of reports to PDF and XML files. | |
| | 34. | The proposed solution must provide the centralized administration of backup storages and quarantine on all network resources where the anti-malware software is installed. | |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <p>35. The proposed solution must provide the creation of internal accounts to authenticate administrators on the administration server.</p> <p>36. The proposed solution must provide the creation of an administration system backup copy with the help of integrated administration system tools.</p> <p>37. The proposed solution must support Windows Failover Cluster.</p> <p>38. The proposed solution must have a built-in clustering feature.</p> <p>39. The proposed solution must include some form of system to control virus epidemics.</p> <p>40. The proposed solution must include Role Based Access Control (RBAC), and this must allow restrictions to be replicated throughout the management servers in the hierarchy.</p> <p>41. The proposed solution's management server must include pre-defined security roles for the Auditor, Supervisor and Security Officer.</p> <p>42. The proposed solution must have ability manage mobile devices through remote commands.</p> <p>43. The proposed solution must have ability to delete downloaded updates.</p> <p>44. The proposed solution must generate Managing Administration Server updates from the application interface.</p> <p>45. The proposed solution must enable the selection of an update agent for client computers based on a network analysis.</p> <p>46. The proposed solution must clearly show information about the distribution of vulnerabilities across managed computers.</p> <p>47. The proposed solution's management server interface must support the Arabic language.</p> <p>48. The proposed solution's management server must maintain a revision history of the policies, tasks, packages, management groups created, so that modifications to a particular policy/task can be reviewed.</p> <p>49. The proposed solution's management server must have functionality to create multiple profiles within a protection policy with different protection settings that can be simultaneously active on a single/multiple devices based on the following activation rules:</p> | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | <ul style="list-style-type: none"> • Device status • Tags • Active directory • Device owners • Hardware | |
| | <p>50. The proposed solution must support following notification delivery channels:</p> <ul style="list-style-type: none"> • Email • Syslog • SMS • SIEM | |
| | <p>51. The proposed solution must have the ability to define an IP address range, in order to limit client traffic towards the management server based on time and speed.</p> | |
| | <p>52. The proposed solution must have the ability to perform inventory on scripts and .dll files.</p> | |
| | <p>53. The proposed solution must have the ability to tag/mark computers based on:</p> <ul style="list-style-type: none"> • Network Attributes <ul style="list-style-type: none"> ◦ Name ◦ Domain and/or Domain Suffix ◦ IP address ◦ IP address to management server • Location in Active Directory <ul style="list-style-type: none"> ◦ Organizational Unit ◦ Group • Operating System <ul style="list-style-type: none"> ◦ Type and Version ◦ Architecture ◦ Service Pack number • Virtual Architecture • Application registry <ul style="list-style-type: none"> ◦ Application name ◦ Application version ◦ Manufacturer | |
| | <p>54. The proposed solution must have the ability to create/define settings based on a computer's location in the network, rather than the group to which it belongs in the management server.</p> | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--|
| | 55. The proposed solution must have the functionality to add a unidirectional connection mediator between the management server and the endpoint connecting over the internet/public network. | |
| | 56. The proposed solution must allow the administrator to define restricted settings in policy/profile settings, so that a virus scan task can be triggered automatically when a certain number of viruses are detected over defined amount of time. The values for the number of viruses and timescale must be configurable. | |
| | 57. The proposed solution must have a customizable dashboard generating and displaying real time statistics for endpoints. | |
| | 58. The proposed solution must allow the administrator to customize reports. | |
| | 59. The proposed solution must have the functionality to detect non-persistent virtual machines and automatically delete them and their related data from the management server when powered off. | |
| | 60. The proposed solution must enable the administrator to set a period of time after which a computer not connected to the management server, and its related data are automatically deleted from the server. | |
| | <p>61. The proposed solution must allow the administrator to create categories/groups of application based on:</p> <ul style="list-style-type: none"> • Application Name • Application Path • Application Metadata • Application Digital certificate • Vendor pre-defined application categories • SHA • Reference computers <p>to allow/deny their execution on endpoints.</p> | |
| | 62. The proposed solution must allow the administrator to define different status change conditions for groups of endpoints in the management server. | |
| | 63. The proposed solution must allow the administrator to add custom/3rd party endpoint management tools into the management server. | |
| | 64. The proposed solution must have a built-in feature/module to remotely collect the data needed for troubleshooting from the endpoints, without requiring physical access. | |

| Item # | | TECHNICAL SPECIFICATIONS | |
|--------|--|---|--|
| | | 65. The proposed solution must allow the administrator to create a Connection Tunnel between a remote client device and the management server if the port used for connection to the management server is not available on the device. | |
| | | 66. Suggest solution must have built-in functionality to remotely connect to the endpoint using Windows Desktop Sharing Technology. In addition, the solution must be able to maintain the auditing of administrator actions during the session. | |
| | | 67. The proposed solution must have a feature to create a structure of administration groups using the Groups hierarchy, based on the following data: <ul style="list-style-type: none"> • structures of Windows domains and workgroups • structures of Active Directory groups • contents of a text file created by the administrator manually | |
| | | 68. The proposed solution must be able to retrieve information about the equipment detected during a network poll. The resulting inventory should cover all equipment connected to the organization's network. <p>Information about the equipment should update after each new network poll. The list of detected equipment should cover the following:</p> <ul style="list-style-type: none"> • devices • mobile devices • network devices • virtual devices • OEM components • computer peripherals • connected devices • VoIP phones • network repositories <p>The administrator must be able to add new devices to the equipment list manually or edit information about equipment that already exists on the network.</p> <p>'Device is Written Off' functionality must be available, so that such devices are not displayed in the equipment list.</p> | |
| | | 69. The proposed solution must incorporate a single distribution/relay agent to support at least 10,000 | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|---|
| | <p>endpoints for the delivery of protection, updates, patches, and installation packages to remote sites.</p> <p>70. The proposed solution must incorporate a single distribution/relay agent to relay/transfer or proxy threat reputation requests from endpoints to the management server.</p> <p>71. The proposed solution must support the download of differential files rather than full update packages.</p> <p>72. The proposed solution must support OPEN API, and include guidelines for integration with 3rd party external systems.</p> <p>73. The proposed solution must include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.</p> <p>74. The proposed solution must include Role Based Access Control (RBAC) with customizable predefined roles.</p> <p>75. The proposed solution's primary/parent management server must be able to relay updates and cloud reputation services.</p> <p>76. The proposed solution's reports must include information about each threat and the technology that detected it.</p> <p>77. The proposed solution report must include details about which endpoint protection components are, or are not, installed on client devices, regardless of the protection profile applied/existing for these devices.</p> <p>78. The proposed solution's primary management server must be able to retrieve detailed information reporting on the health status etc. of managed endpoints from the secondary management servers.</p> <p>79. The proposed solution must include the option for the customer to either deploy an on-premises management console, or use the vendor-provided cloud-based management console.</p> <p>80. The proposed solution must be able to integrate with the vendor's cloud-based management console for endpoint management at no additional cost.</p> <p>81. The proposed solution must enable swift migration from the on-premises management console to the vendor cloud-based management console.</p> <p>82. The proposed solution must include the following SIEM integration options:</p> |

| Item # | TECHNICAL SPECIFICATIONS | |
|--------|--|--------------------------------|
| | <ul style="list-style-type: none"> • HP (Microfocus) ArcSight • IBM QRadar • Splunk • Syslog <p>83. The proposed solution must include support for cloud-based deployment via:</p> <ul style="list-style-type: none"> • Amazon Web Services • Microsoft Azure | |
| | <p>84. The proposed solution must provide anti-malware database update mechanisms including:</p> <ul style="list-style-type: none"> • Multiple ways of updating, including global communication channels over the HTTPS protocol, shared resource at local network and removable media. • Verification of the integrity and authenticity of updates by means of an electronic digital signature. | |
| | <p>85. The proposed solution must support Single Sign On (SSO) using NTLM and Kerberos.</p> | |
| | <p>86. The solution must be capable of removing the existing endpoint security agent/solution within 8 hours without user intervention, i.e., auto-discover on 300 devices. (As applicable)</p> | |
| | <p>87. The solution must be capable of deploying and installing the endpoint security agents within 8 hours without user intervention, i.e., auto-discover on 300 devices. (As applicable)</p> | |
| | <p>88. The solution must be fully operational within 1 hour after deployment and installation to each device. (As applicable)</p> | |
| | Documentation <ol style="list-style-type: none"> 1. Requirements for solution documentation. Documentation for all anti-malware software, including administration tools, should include the following documents: <ul style="list-style-type: none"> Online Help for Administrators Online Help for implementation best practices | Statement of Compliance |
| | <ol style="list-style-type: none"> 2. The anti-malware software documentation provided should describe in detail the processes of installation, configuration and use of the anti-malware software. | |



| Item # | TECHNICAL SPECIFICATIONS | |
|--------|---|--|
| | | |
| 11 | <p><u>General Terms and Conditions</u></p> <p>A. Terms</p> <ol style="list-style-type: none"> 1. The request(s) for payment shall be made to UCPBS in writing, accompanied by an invoice describing, as appropriate, the output/report delivered and/or services performed, and by submission of other required documents and obligations stipulated in this contract. 2. All payments shall be VAT-inclusive and subject to 2% expanded withholding tax and 5% Final VAT (if supplier is VAT-registered with BIR). 3. Since the payment/s shall be subject to the usual government accounting and auditing requirements, the Supplier is expected to be familiar with the Government Accounting and Auditing Manual (GAAM). 4. Retention Payment. <p>A retention payment of one (1) percent shall be withheld by UCPBS. It shall be based on the total amount due to the Supplier prior to any deduction and shall be retained from every progress payment.</p> <p>The total ‘retention money’ shall be due for release upon approval/ acceptance of the Final Report/Acceptance. The Supplier may, however, request the substitution of the retention money for each progress billing with irrevocable standby letters of credit from a commercial bank, bank guarantees, or surety bonds callable on demand, of amounts equivalent to the retention money substituted for and acceptable to UCPBS provided that the Project is on schedule and is satisfactorily undertaken. Otherwise, the one (1) percent retention shall be made. Said irrevocable standby letters of credit, bank guarantees and/or surety bonds, to be posted in favor of UCPBS shall be valid for the duration of the contract.</p> <p>B. Warranties</p> <p>Warranty on Parts</p> <p>The Supplier warrants that the replacement part as specified under Technical Specifications Section 5 (Support Coverage) will be free from defects in material or workmanship for a period of three (3) months from the date the part was installed on the covered component detailed in Technical Specifications Section 3 (Covered Components).</p> <p>Warranty on Services</p> <p>The Supplier warrants that the activities included in the Solution will be executed using the degree of skill and care required by customarily accepted good professional and technical practices. If the services provided did not conform to the terms and conditions specified under this TOR, the Supplier shall re-perform such services at no additional cost to the Bank.</p> <p>C. Incidental Services (Indicate, if any)</p> <ol style="list-style-type: none"> 1. Incidental Services, if any, shall be as described in Technical Specs. 2. Such incidental services may include the following: Project/ Solution documentation, knowledge transfer (trainings), systems and tools to facilitate monitoring of Project/Solution tasks, trouble tickets, incident reports, and inventory. | |



| Item # | TECHNICAL SPECIFICATIONS |
|--------|--|
| | <p>D. Termination</p> <p>UCPBS may, subject to five (5) days' advance notice, terminate the contract with the Supplier or cancel the purchase order (PO) it issued to the Supplier, on any of the following grounds:</p> <ul style="list-style-type: none"> 3. Misrepresentation by the selected supplier of any matter which UCPBS deems material, or 4. Failure by the selected supplier to deliver the goods and services to the satisfaction of UCPBS on the Delivery Schedule. <p>Notwithstanding any provision in the General and Special Conditions of Contract, UCPBS may pre-terminate this Contract subject to a notice to the Supplier within thirty (30) days prior to the effective date of pre-termination.</p> <p>E. Liquidated Damages</p> <p>When the supplier fails to satisfactorily deliver goods and/or services under this Terms of Reference (TOR) within the specified delivery schedule, inclusive of duly granted time extension, if any, the supplier shall be liable for damages in an amount equal to one-tenth (1/10) of one percent (1%) of the contract price for delivery for every day of delay until such goods are finally delivered and accepted by UCPBS. Such amount shall be deducted from any money due or which may become due to the Supplier.</p> <p>If UCPBS opts to terminate the contact or cancel the PO, the Supplier shall be liable to pay UCPBS liquidated damages in an amount computed, as follows:</p> <ul style="list-style-type: none"> (a) In case of misrepresentation, one-tenth (1/10) of one percent (1%) of the contract price per day starting from the date of UCPBS discovery of the misrepresentation until the effective date of termination of the contract or cancellation of the PO, and/or (b) In case of delay in the delivery of the goods and/or services to the satisfaction of UCPBS, one-tenth (1/10) pf one percent (1%) of the contract price per day starting from the Delivery schedule until the effective date of termination of the contract or cancellation of the PO. <p>In case the selected supplier is guilty of both misrepresentation and delay, the liquidated damages shall be computed using the formula of either (a) or (b), whichever is higher.</p> <p>The Supplier shall pay UCPBS the liquidated damages under this Section within five (5) days from the effective date of the termination of the contract or cancellation of the PO without need of demand.</p> <p>F. No Employer-Employee Relationship</p> <p>Nothing in this TOR shall be construed as constituting an employer and employee relationship between UCPBS and the selected supplier, his/her/its employees and/or representatives.</p> <p>G. Confidentiality of Information</p> <p>The selected supplier shall observe the provisions of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, in the performance of its obligations under this TOR.</p> |



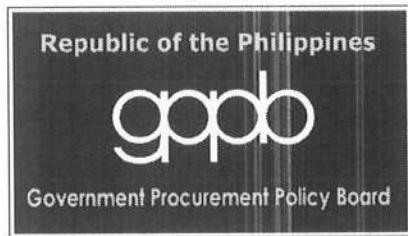
I hereby commit to comply and deliver the above requirements.

Name of Company (in print)

Signature of Company Authorized Representative

Name and Designation (in print)

Date

A handwritten signature is written in black ink, appearing to be a stylized "GPPB".