PHILIPPINE BIDDING DOCUMENTS

(As Harmonized with Development Partners)

Procurement of GOODS

Sixth Edition

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES

BID REFERENCE NO. G-2025-20

August 2025

Table of Contents

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

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

1. The ***Development Bank of the Philippines***, through the ***Corporate Budget***, intends to apply the sum of ***One Hundred Sixty-Five Million Pesos (PhP 165,000,000.00) for three years or Fifty-Five Million Pesos (PhP55,000,000.00) per year****, inclusive of all applicable taxes* being the Approved Budget for the Contract (ABC) to payments for the contract for the above-cited project.

2. The ***Development Bank of the Philippines*** now invites bids for the above-cited procurement project. Bids received in excess of the ABC shall be automatically rejected at bid opening.

3. The contract of the project shall cover the delivery, installation, configuration, and subscription including training, maintenance and after-sales support which will commence upon receipt of the Notice to Proceed by the bidder. License subscription will start upon issuance of the Certificate of Acceptance by DBP.

4. Bidders must have completed a contract similar to the project **within the last five (5) years** from the date of submission and receipt of bids, with the following options:

Options	***SLCC Requirement***
1	**Single contract** equivalent to at least fifty percent (50%) of the ABC for one year; OR
2	**At least two (2) similar contracts**, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for one year.

   A contract similar to the project refers to any Cybersecurity Managed Services solutions which includes the delivery, subscription, installation, and/or maintenance and support. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

5. 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.

6. Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA No. 5183.

7. Prospective Bidders may obtain further information from *the* ***Development Bank of the Philippines*** and inspect the Bidding Documents at the address given below Mondays to Fridays from 9:00 AM to 4:30 PM.

8. A complete set of Bidding Documents may be acquired by interested Bidders 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 Fifty Thousand Pesos (PhP 50,000.00).*** The Procuring Entity shall allow the bidder to present its proof of payment for the fees *via physical presentation of Official Receipt (OR) (original).* Bidders shall also be given the printed format of the Bidding Documents provided that bidders shall pay the applicable Bidding Documents Fee at least the day before the deadline for submission of their bids.

BAC Secretariat Unit - Procurement and Inventory Management Department (PIMD), 6th Floor, Development Bank of the Philippines (DBP)-Head Office, Sen. Gil Puyat Ave., cor. Makati Ave., Makati City

9. The following is the schedule of bidding activities:

Particulars	Date	Venue
Issuance and Availability of Bidding Documents	**Starting 12 August 2025** **9:00 AM to 3:00 PM only** **(excluding weekends and holidays)**	6/F BAC Secretariat, DBP Head Office, Makati City
Pre-Bid Conference*	**20 August 2025 (Wednesday)** **9:30 AM**	12/F Suite 5, DBP Head Office, Makati City
Submission of Eligibility and Technical Documents, and Financial Proposals	**3 September 2025 (Wednesday)** **ON OR BEFORE 9:00 AM**	6/F BAC Secretariat, DBP Head Office, Makati City
Opening of Eligibility and Technical Documents, and Financial Proposals	**3 September 2025 (Wednesday)** **9:30 AM**	12/F Suite 5, DBP Head Office, Makati City

Note: The Pre-bid Conference shall be open to all interested parties.* ***Bidders may attend the Pre-bid Conference and Bid Opening through videoconferencing via Zoom Meeting App. Bidders who wish to attend/participate via Zoom Meeting must coordinate with the BAC Secretariat through email at least one (1) day before the scheduled bid activity and provide their contact information (name of company, name of representative, email address, contact number)**. Bidders are advised to send their authorized technical and/or administrative representatives who will prepare the bid documents to ensure completeness and compliance of bids.*

10. Bids must be duly received by the BAC Secretariat through (i) manual submission at the office address indicated above **OR** via (ii) online or electronic submission **on or before deadline as specified on the above schedule. Late bids shall not be accepted.**

11. Electronic bids shall only be submitted through the BAC's Microsoft OneDrive, as the official electronic/online submission facility. Bidders shall inform and coordinate with the BAC Secretariat (bacsecretariat@dbp.ph) on their intent to submit their bids online at least one (1) day before the scheduled deadline of submission. **Bids which are not submitted through MS OneDrive and/or not password-protected shall be disqualified.** Please refer to the Bid Data Sheet for the detailed guidelines and procedure for electronic/online submission.

12. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 14.

13. The ***Development Bank of the Philippines*** 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.

14. For further information, please refer to:

    DBP Bids and Awards Committee Secretariat
    6/F Procurement and Inventory Management Department
    DBP Head Office, Sen. Gil J. Puyat corner
    Makati Avenue, Makati City
    Trunkline: (+632) 8818-9511 local 2610 or 2606
    Email: bacsecretariat@dbp.ph
    Bid Reference No. G-2025-20

15. You may visit the following websites for downloading of Bidding Documents:
    - DBP website: *https://www.dbp.ph/invitations-to-bid/*
    - PhilGEPS website: *https://philgeps.gov.ph/*

(SIGNED)
DBP Bids and Awards Committee

REMINDER TO BIDDERS:

- Please be informed that DBP exercises Zero Tolerance for all types of fraud including illegal practices, corruption and malpractices. DBP officers and employees shall act ethically and lawfully in all transactions and dealing with stakeholders avoiding any appearance of irregularity that could erode the trust and confidence in the Bank as an institution and as the government as a whole.
- DBP cautions the public in dealing with individuals claiming association with the Bank, especially those posing as BAC members for any form of monetary solicitation or support. DBP does not condone illegal acts and disowns any responsibility for transactions made with unauthorized individuals.

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, *Development Bank of the Philippines* wishes to receive Bids for the **ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES**, Bid Reference No. G-2025-20.

The Procurement Project (referred to herein as "Project") consists of one lot, 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 in the amount of ***One Hundred Sixty-Five Million Pesos (PhP 165,000,000.00) for three years or Fifty-Five Million Pesos (PhP55,000,000.00) per year)***, *inclusive of all applicable taxes.*

2.2. The source of funding is the Development Bank of the Philippines.

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 limited to 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. The Bidder must have completed either of the following contracts within the last five (5) years, with the following options

Options	***SLCC Requirement***
1	**Single contract** equivalent to at least fifty percent (50%) of the ABC for one year; OR
2	**At least two (2) similar contracts**, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for one year.

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 **ITB** Clause 18.

7. Subcontracts

7.1. The Bidder may subcontract portions of the Project to the extent allowed by the Procuring Entity as stated herein, but in no case more than twenty percent (20%) of the Project.

The Procuring Entity has prescribed that: **Subcontracting is not allowed**.

7.2. *[If Procuring Entity has determined that subcontracting is allowed during the bidding, state:]*The Bidder must submit together with its Bid the documentary requirements of the subcontractor(s) complying with the eligibility criteria stated in **ITB** Clause 5 in accordance with Section 23.4 of the 2016 revised IRR of RA No. 9184 pursuant to Section 23.1 thereof.

7.3. *[If subcontracting is allowed during the contract implementation stage, state:]* The Supplier may identify its subcontractor during the contract implementation stage. Subcontractors identified during the bidding may be changed during the implementation of this Contract. Subcontractors must submit the documentary requirements under Section 23.1 of the 2016 revised IRR of RA No. 9184 and comply with the eligibility criteria specified in **ITB** Clause 5 to the implementing or end-user unit.

7.4. Subcontracting of any portion of the Project does not relieve the Supplier of any liability or obligation under the Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants, or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants, or workmen.

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time and either at its physical address **12th Floor, Suite 5, DBP Head Office, Makati and/or through videoconferencing/webcasting as indicated in paragraph 8 of the IB.**

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 Eligibility, Technical and Financial Documents)**.

10.2. The Bidder's SLCC as indicated in **ITB** Clause5.3 should have been completed ***within the last five (5) 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 Eligibility, 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 **IB** 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 Declaration[1] 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 until *One Hundred Twenty (120) Calendar Days from the Date of the Bid Opening.* Any Bid not accompanied by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

[1] 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.

15. Sealing and Marking of Bids

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

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 or through online submission as indicated in paragraph 7 of the **IB.**

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 **IB**. 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.

[Include the following options if Framework Agreement will be used:]

a. In the case of single-year Framework Agreement, the Lowest Calculated Bid shall be determined outright after the detailed evaluation;

b. For multi-year Framework Agreement, the determination of the eligibility and the compliance of bidders with the technical and financial aspects of the projects shall be initially made by the BAC, in accordance with Item 7.4.2 of the Guidelines on the Use of Framework Agreement.

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 **ITB** 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 **<u>as one lot.</u>**

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. 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**.

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

<table>
<tr><th>ITB Clause</th><th></th></tr>
<tr><td>5.3</td><td>For this purpose, contracts similar to the Project shall be:

A contract similar to the project refers to <b>any Cybersecurity Managed Services solutions which includes the delivery, subscription, installation, and/or maintenance and support</b>.

a. Completed within the last five (5) years prior to the deadline for the submission and receipt of bids contracts with the following options:

<table>
<tr><th><i>Options</i></th><th><i>SLCC Requirement</i></th></tr>
<tr><td>1</td><td><b>Single contract</b> equivalent to at least fifty percent (50%) of the ABC for one year; OR</td></tr>
<tr><td>2</td><td><b>At least two (2) similar contracts</b>, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for one year.</td></tr>
</table>
</td></tr>
<tr><td>7.1</td><td><i>Not applicable</i>

<i>[Specify the portions of Goods to be subcontracted, which shall not be a significant or material component of the Project as determined by the Procuring Entity.]</i></td></tr>
<tr><td>8</td><td>The <b>Development Bank of the Philippines</b> will hold a Pre-bid conference for this Project on:

Date: <b>20 August 2025 (Wednesday); 9:30 AM</b>

Venue: 12th floor, Suite 5, DBP Head Office, Makati City <b>and/or through videoconferencing/webcasting as indicated in paragraph 8 of the Invitation to Bid (IB).</b>

<b>Conduct of Pre-bid Conference:</b>

Bidders shall be allowed to participate during the conduct of Pre-bid Conference via Zoom Meeting App. Although attendance during the Pre-bid Conference is not mandatory, prospective bidders are encouraged to attend to fully understand the Bank’s requirements through its Technical Specifications, Scope of Works or Terms of Reference and other contents of the Bidding Documents.

a. Non-attendance of a prospective bidder during the Pre-bid Conference will in no way prejudice its bid. However<b>, it is the sole responsibility of the bidder to know the changes and/or amendments to the Bidding Documents as recorded in the minutes of the pre-bid conference and the issuance of the Supplemental/Bid Bulletin.</b>

b. All prospective bidders shall be guided by the following:

b.1 All prospective bidders who will attend the Pre-bid Conference must use the Zoom Meeting App and must coordinate with the BAC</td></tr>
</table>

	Secretariat through email **at least one (1) day before the scheduled Pre-bid Conference and provide their contact information**: ✓ Complete name of the representative ✓ Complete name of the company ✓ Registered e-mail address ✓ Mobile/cell phone numbers b.2 The BAC Secretariat shall send an invite to all prospective bidders through their respective e-mails who desire to join/participate in the Pre-bid Conference using Zoom Meeting at least one (1) day before the said activity. b.3 The BAC Secretariat shall call all prospective bidders using Zoom Meeting on the respective time slots for a specific procurement project; b.4 The Chairman, or in her absence, the First Vice Chairperson or the Second Vice Chairperson, shall acknowledge all prospective bidders who are present via Zoom Meeting; b.5 Bidders shall turn on their video cameras at all times or during the Pre-bid Conference and Opening of Bids for transparency and recording purposes. b.6 If in case a bidder was not able to join the Pre-bid Conference, they may send their clarifications or queries to the Secretariat through e-mail. All clarifications or queries sent via e-mail including those that were discussed during the Pre-bid Conference shall be properly recorded and shall be included and addressed in the Supplemental Bid Bulletin; b.7 Prospective bidders need not to have their account/e-mails registered in the Office 365. However, bidder must still download the Zoom Meeting App.
12	The price of the Goods shall be quoted DDP *[state place of destination]* or the applicable International Commercial Terms (INCOTERMS) for this Project.
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 *[two percent (2%) of ABC]*, if bid security is in cash, cashier's/manager's check, bank draft/guarantee or irrevocable letter of credit; b. The amount of not less than *[five percent (5%) of ABC],* if bid security is in Surety Bond; c. No required percentage, if bid security is in the form of Bid Securing Declaration.

Approved Budget for the Contract (ABC)	Cashier's/manager's check, Bank draft/guarantee or irrevocable letter of credit (2% of ABC)	Surety Bond (5% of ABC)	Bid Securing Declaration
165,000,000.00	**3,300,000.00**	**8,250,000.00**	**No required percentage**

15 **<u>For Manual Submission of Bids:</u>**

Each bidder shall submit one (1) original and two (2) copies of the first and second components of its bid.

Bidders shall submit their bids through their duly authorized representative enclosed in sealed envelopes:

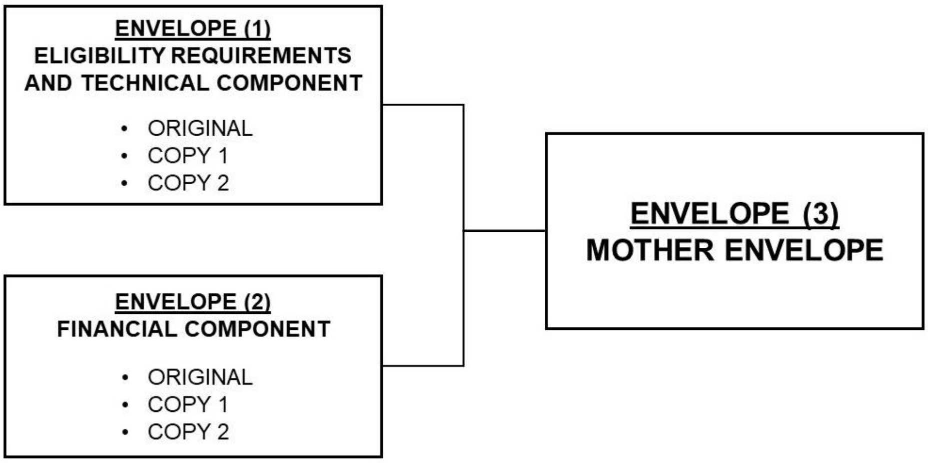
a. The first sealed envelope "**ENVELOPE (1)**" shall contain the folder/binder of the Eligibility Requirements and Technical Component of the bid; prepared in three copies labeled as follows:

- ORIGINAL – Eligibility Requirements and Technical Component
- COPY 1 – Eligibility Requirements and Technical Component
- COPY 2 – Eligibility Requirements and Technical Component

b. The next sealed envelope "**ENVELOPE (2)**" shall contain the folder/binder of the Financial Component of the bid; prepared in three copies labeled as follows:

- ORIGINAL – Financial Component
- COPY 1 – Financial Component
- COPY 2 – Financial Component

c. "ENVELOPE (1)" and "ENVELOPE (2)" shall then be enclosed in a single mother envelope/package/box, which must be duly labeled, signed, and sealed.



d. All envelopes "ENVELOPE (1)", "ENVELOPE (2)", and the MOTHER ENVELOPE shall indicate the following as its **outer label**:

- addressed to DBP-BAC
- name and address of the bidder in all capital letters
- name of the project to be bid in all capital letters
- bear the specific reference number for the project
- bear a warning "DO NOT OPEN BEFORE…" the date and time for the opening of bids

TO : **THE BIDS AND AWARDS COMMITTEE**
DEVELOPMENT BANK OF THE PHILIPPINES (DBP)
FROM : ____
(*Name of Bidder in All Capital Letters)*
ADDRESS: ____
(Address of Bidder in All Capital Letters)
PROJECT : ____

BID REFERENCE NO : ______________________________
(In Capital Letters, Indicate the Phrase):
"DO NOT OPEN BEFORE: (<u>DATE AND TIME OF OPENING OF BIDS</u>)"

<u>For Online/Electronic Submission of Bids:</u>

Proper labelling of bids (<u>for ELECTRONIC BID SUBMISSION</u>)

All bidders must upload their bids/archived files in their respective folders as illustrated below:

1) For the first envelope/archived file containing the Eligibility and Technical Proposals:

- (Name of Company/Office/Bidder)_FOLDER 1_ELIGIBILITY AND TECHNICAL COMPONENT_BID

e.g. ABC Company_FOLDER 1_ELIGIBILITY AND TECHNICAL COMPONENT_BID

2) For the second envelope/archived file containing the Financial Proposals:

- (Name of Company/Office/Bidder)_FOLDER 2_FINANCIAL COMPONENT_BID

e.g. ABC Company_FOLDER 2_FINANCIAL COMPONENT_BID

Manner of Submission of Bids

The BAC shall adopt the following procedure in the submission and receipt of bids:

Manual Submission:

a. Bidders shall be permitted to submit bids through actual submission by submitting the printed copies which must still be compliant with the two-envelope system and the sealing and marking of bids under Section 25 of the Republic Act No. 9184 and its 2016 Revised Implementing Rules and Regulations (IRR);

b. Bidders shall submit the printed copies of their bid proposals preferably at least one (1) day before the deadline for the submission and receipt of bids;

c. Bidders may send another representative to submit their bid proposals;

d. The bidder or its representative shall coordinate with the Secretariat in submitting their bids. Bidders or its representative shall present to the Secretariat the transmittal page containing the Checklist of Requirements attached in the Bidding Documents, or if in case a Supplemental Bid Bulletin was issued, the transmittal page containing the Revised Checklist of Requirements, in which a date and time stamp shall be given as a proof on the submission and receipt of bids. The date and time stamp shall serve as the reference of the BAC and the bidders during the Opening of the Bids;

e. The Secretariat shall be the sole custodian and shall be responsible in safekeeping the bid proposals;

Electronic Submission:

a. Bidders shall submit their bid proposals via e-mail electronic format/e-mail provided that it shall comply with the following requirements:

a.1 uses a two-factor security procedure consisting of an archive format compression and password protection to ensure the security, integrity and confidentiality of the bids submitted;

a.2 allows access to a password-protected Bidding Documents on opening date and time. The passwords for accessing the file will be disclosed by the Bidders only during the actual bid opening which may be done in person or face-to-face through videoconferencing, webcasting or similar technology; and

a.3 capable of generating an audit trail of transactions to ensure the security, integrity and authenticity of bid submissions.

b. Bidders shall comply with the required and proper labelling of bids provided in ***Clause 15 of Bid Data Sheet (BDS).***

c. Bidders shall submit their bid proposals using the following format:

✓ The following documents must be saved in PDF file format:

	• Eligibility (Legal, Technical and Financial) and Technical Documents (First Envelope); and • Financial Proposals (Second Envelope) ✓ Must be in archived/.zip file format. ***Note:*** *.RAR is not recommended*. ✓ Shall be labelled as "Name of the Company/Office/Bidder_ ELIGIBILITY AND TECHNICAL/FINANCIAL_BID" ✓ Password encrypted **For the detailed procedures on how to create and encrypt password on archive files, please refer to *PAGE 49* of this Guidelines**. d. The BAC shall use Microsoft Office 365 OneDrive as the platform/facility for the electronic submission of bids; e. Bidders shall inform/notify the BAC Secretariat through email at bacsecretariat@dbp.ph, at least one (1) day prior to the deadline of submission and receipt of bids, their intent to submit their bids online. The BAC Secretariat shall then send to the bidders the link of the MS OneDrive folder where the bidders shall upload their electronic bids. f. Upon receipt of the bids containing the first and second envelopes, the BAC through its Secretariat shall send a "Bid Receipt" page for the official date and time of submission which can be saved or printed by the bidder; g. A bidder may modify its bid, provided that this is done before the deadline for the submission and receipt of bids. Bidders shall send another bid equally secured, properly identified, and labelled as a "modification" of the one previously submitted. The time indicated in the latest "Bid Receipt" page generated shall be the official time of submission. Bids submitted after the deadline shall not be accepted. h. Bids which are not submitted through BAC's MS OneDrive and/or not password-protected shall be disqualified. i. Bids that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified. j. The use of the aforesaid online or electronic bid submission shall be allowed until such time the online bidding facility under the PhilGEPS becomes fully operational.
16	The address for submission of bids is: **Development Bank of the Philippines - Head Office** **Bids and Awards Committee (BAC) Secretariat** 6th floor, BAC Secretariat, Procurement and Inventory Management Department (PIMD), Sen. Gil Puyat Ave., corner Makati Ave., Makati City

	The deadline for submission of bids is: **3 September 2025 (Wednesday); “ON OR BEFORE” 9:00 AM**
17	The place of bid opening is: **Development Bank of the Philippines-Head Office** 12th floor, Suite 5, DBP Head Office, Makati City, or via Zoom Meeting app The date and time of bid opening is: **3 September 2025 (Wednesday); 9:30 AM**
19.3	*No further instruction* *[In case the Project will be awarded by lot, list the grouping of lots by specifying the group title, items, and the quantity for every identified lot, and the corresponding ABC for each lot.]* *[In case the project will be awarded by item, list each item indicating its quantity and ABC.]*
20.2	*No further instruction* *[List here any licenses and permits relevant to the Project and the corresponding law requiring it.]*
21.2	*No further instruction* *[List here any additional contract documents relevant to the Project that may be required by existing laws and/or the Procuring Entity.]*

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

Special Conditions of Contract

GCC Clause	
1	*No further instruction* *<u>Please refer to the Draft Contract per Section XII of this Bidding Documents</u>* **Delivery and Documents –** 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: *[For Goods supplied from abroad, state:]* “The delivery terms applicable to the Contract are DDP delivered [*indicate place of destination*]. In accordance with INCOTERMS.” *[For Goods supplied from within the Philippines, state:*] “The delivery terms applicable to this Contract are delivered *[indicate place of destination].* Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination.” Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity’s Representative at the Project Site is *[indicate name(s)].* **Incidental Services –** The Supplier is required to provide all of the following services, including additional services, if any, specified in Section VI. Schedule of Requirements: *Select appropriate requirements and delete the rest.* a. performance or supervision of on-site assembly and/or start-up of the supplied Goods; b. furnishing of tools required for assembly and/or maintenance of the supplied Goods; c. furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods;
	d. performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and

e. training of the Procuring Entity's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied Goods.

f. *[Specify additional incidental service requirements, as needed.]*

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.

Spare Parts –

The Supplier is required to provide all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier:

Select appropriate requirements and delete the rest.

a. such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and

b. in the event of termination of production of the spare parts:

   i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and

   ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested.

The spare parts and other components required are listed in **Section VI (Schedule of Requirements)** and the cost thereof are included in the contract price.

The Supplier shall carry sufficient inventories to assure ex-stock supply of consumable spare parts or components for the Goods for a period of [*indicate here the time period specified. If not used indicate a time period of three times the warranty period*].

Spare parts or components shall be supplied as promptly as possible, but in any case, within [*insert appropriate time period*] months of placing the order.

Packaging –

The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit.

The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity.

The outer packaging must be clearly marked on at least four (4) sides as follows:

Name of the Procuring Entity

Name of the Supplier

Contract Description

Final Destination

Gross weight

Any special lifting instructions

Any special handling instructions

Any relevant HAZCHEM classifications

A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging.

Transportation –

Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract, shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price.

Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price.

	Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination. **Intellectual Property Rights –** 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.
2.2	*Payment shall be based on actual services rendered.* ***The bidder declared as Lowest or Single Calculated and Responsive Bid must open an account with DBP upon issuance of Notice of Award for payment purposes (in case no account with DBP yet).***
4	No further instruction The inspections and tests that will be conducted are: *[Indicate the applicable inspections and tests]*

Section VI. Schedule of Requirements

The contract of the project shall cover the delivery, subscription, installation, configuration, testing and commissioning including training, maintenance and After Sales Support which will commence upon receipt of the Notice to Proceed by the bidder. License subscription will start upon issuance of the Certificate of Acceptance by DBP.

Please refer to Form 9 – Technical Specifications for the complete project requirements.

Section VII. Technical Specifications

Technical Specifications

Please refer to FORM 9 of this Bidding Documents for the Technical Specifications (TS) / Terms of Reference (TOR)

Section VIII. Checklist of Eligibility, Technical and Financial Documents

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

TRANSMITTAL FORM

CHECKLIST OF REQUIREMENTS FOR BIDDERS

Note: Please fill-out this form and submit directly to the BAC Secretariat outside of the sealed envelopes.

FOR MACHINE STAMP (OFFICIAL TIME) BY THE DBP BAC SECRETARIAT
Received:

Name of Bidder:____

Complete Address:____

Submitted by:____

Landline:__________________ Email:____

Item	FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)
LEGAL ELIGIBILITY DOCUMENTS	
TAB 1	If the bidder is a joint venture (JV): **a. If bidding as a formed JV:** Submit the existing valid, duly accomplished, signed and notarized JV Agreement (JVA). The JVA must specifically indicate among others, the following: the partner company that will represent the JV, the shareholdings of each partner company in the JV (to determine which partner company and its nationality has the controlling majority share), and the share of each partner company in the JV. Moreover, please likewise note: 1) If the JV is incorporated or registered with the relevant government agency, all documents listed in this checklist must be under the JV's name and shall submit the PhilGEPS Certificate of Registration under Platinum Category also under the JV's name. 2) If the JV is unincorporated, the PhilGEPS Certificate of Registration under Platinum Membership shall be submitted by each of the JV partners, while submission of the technical and financial eligibility documents (Tab 4 onwards) by any one of the JV partners constitutes collective compliance. **b. If bidding as a JV that is yet to be formed: Submit duly notarized Agreement to Enter into Joint Venture** (***Template per FORM 1***)**.** Please likewise note: PhilGEPS Certificate of Registration under Platinum Membership shall be submitted by each of the JV partners, while submission of the technical and financial documents (Tab 4 onwards) by any one of the JV partners constitutes collective compliance.

Item	**FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)**
	Please refer to ***FORM 1-A*** and ***FORM 1-B*** for the sample Secretary's Certificate for each of the JV Partners. *Each JV partner must submit its duly notarized Special Power of Attorney or Secretary's Certificate, whichever is applicable, indicating therein the following:* *1. The designated/authorized representative who will sign the Joint Venture Agreement (JVA) or the Protocol to Enter into a JVA;* *2. That they are duly authorized to participate in the bidding as a JV;* *3. The authorized Lead Company to represent the JV;* *4. The person designated as the duly authorized representative of the corporation to the JV, sign the bid proposals/bidding documents, and sign the ensuing contract with DBP.* In case a JV partner is a sole proprietorship and the principal/proprietor opts to designate a representative, FORM 2-A shall be customized to include provisions such as the authority to sign the Protocol/Undertaking to enter a JVA.
TAB 2	Proof of appointment/authority of bidder's representative: a. **Duly notarized Special Power of Attorney** (if the bidder is a sole proprietorship and opts to designate a representative) - ***Template per FORM 2-A*** OR b. **Duly notarized Secretary's Certificate** (if the bidder is a corporation, partnership, cooperative, or joint venture) - ***Template per FORM 2-B*** **In case there are more than one appointed/designated representatives, bidders must tick ONE of the checkboxes provided in the form to identify if acting ANY ONE OF THE SIGNATORIES, ALL OF THE SIGNATORIES, or ANY (NUMBER) OF THE SIGNATORIES.** **FAILURE TO TICK A CHECKBOX SHALL MEAN THAT ALL AUTHORIZED REPRESENTATIVES ARE SIGNING THE BIDDING FORMS.**
TAB 3	Valid and current Certificate of PhilGEPS Registration (Platinum Membership), in three (3) pages, including Annex "A" or the List of Class "A" Eligibility Documents required to be uploaded and maintained current and updated in PhilGEPS in accordance with section 8.5.2. of the IRR of RA 9184. **Only the current/updated Certificate of PhilGEPS Registration (Platinum Membership) shall be accepted during the opening of bids. Expired Certificate or any of the eligibility documents listed in Annex "A" shall be a ground for failure of the bidder.**
The following are the related provisions/requirements based on GPPB Resolution 15-2021 dated 14 October 2021 regarding submission of valid/current PhilGEPS Certificate of Registration (Platinum Membership):	

<table>
<tr><th>Item</th><th>FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)</th></tr>
<tr><td colspan="2">- ***LIFT the suspension on the implementation of mandatory submission of the PhilGEPS Certificate of Registration (Platinum Membership) in Competitive Bidding and Limited Source Bidding, thus, fully enforcing Sections 8.5.2 and 54.6 of the 2016 revised IRR of RA No. 9184 starting 01 January 2022;***
- ***AMEND Sections 23.1(a)(ii) and 24.1(a)(ii) of the 2016 revised IRR of RA No. 9184 to reflect that the submission of the recently expired Mayor's Permit together with the official receipt as proof that the prospective bidder has applied for renewal within the period prescribed by the concerned local government unit shall be accepted by the PhilGEPS for the purpose of updating the PhilGEPS Certificate of Registration (Platinum Membership) in accordance with Section 8.5.2 of the 2016 revised IRR of RA 9184.***</td></tr>
<tr><td colspan="2">TECHNICAL ELIGIBILITY DOCUMENTS</td></tr>
<tr><td>TAB 4</td><td>Statement by the bidder of **ALL** its ongoing government and/or private contracts (including those awarded but not yet started, if any), whether similar or not similar in nature and complexity to the contract to be bid (include all contracts with the DBP for the said period, if any (***Template per FORM 3***), **duly signed by the bidder's authorized representative.**
Note: For bidders who have no ongoing government and/or private contracts, kindly indicate in their statement "NONE" to comply with the requirement. Bidders will be rated "failed" if no document is submitted or if the document submitted is incomplete or patently insufficient *(per GPPB NPM 094-2013 dtd. 2013-12-19).*
Copies of the NOA, contract, NTP, or equivalent document for each ongoing contract listed in the statement shall be required to be submitted as part of post-qualification of the bidder declared as the Lowest or Single Calculated Bid.</td></tr>
<tr><td>TAB 5</td><td>Statement of single largest completed contract of similar nature (government or private contract) **within the last five (5) years** (***Template per FORM 4***), **duly signed by the bidder's authorized representative**, with the following options:
<table>
<tr><th><i>Options</i></th><th><i>SLCC Requirement</i></th></tr>
<tr><td>1</td><td><b>Single contract</b> equivalent to at least fifty percent (50%) of the ABC for one year; OR</td></tr>
<tr><td>2</td><td><b>At least two (2) similar contracts</b>, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for one year.</td></tr>
</table>
A contract similar to the project refers to **any Cybersecurity Managed Services solutions which includes the delivery, subscription, installation, and/or maintenance and support**.
The identified/listed single largest or at least two completed contract must be supported by the following:
a) Notice of Award (NOA), **OR** Notice to Proceed (NTP), **OR** Contract, **OR** Purchase Order (PO)
AND</td></tr>
</table>

<table>
<tr><th>Item</th><th>FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)</th></tr>
<tr><td></td><td>b) Either one of the following documents:
• Copy of Certificate of Completion **or** Certificate of Acceptance **or** Certificate of Satisfactory Performance issued by the bidder’s client **or** copy of Official Receipt/s **or** Sales Invoice/s issued by the bidder to the client (ORs/SIs must sum up to the full amount of total contract price of completed project).</td></tr>
<tr><td colspan="2">**FINANCIAL ELIGIBILITY DOCUMENTS**</td></tr>
<tr><td>TAB 6</td><td>Completely accomplished computation of Net Financial Contracting Capacity (NFCC) which must be at least equal to the ABC (***Template per FORM 5***), **duly signed by the bidder’s authorized representative.**

1) The values of the bidder’s current assets and current liabilities shall be based on the AFS for **CY 2024.**
2) The value of the NFCC must at least be equal to the ABC of this project.

In case of Joint Venture, the partner responsible to submit the NFCC shall likewise submit the Statement of All its Ongoing Contracts and the latest Audited Financial Statements.

If the prospective bidder opts to submit a committed Line of Credit, it must be at least equal to ten percent (10%) of the ABC to be bid. If issued by a foreign universal or commercial bank, it shall be confirmed or authenticated by a local universal or commercial bank.</td></tr>
<tr><td colspan="2">**TECHNICAL COMPONENT**</td></tr>
<tr><td>TAB 7</td><td>Original Bid Security issued in favor of the Development Bank of the Philippines (must be valid for at least 120 calendar days from the date of bid opening); **either one of the following is acceptable:**

a. Cashier’s/manager’s check issued by a Universal or Commercial Bank (at least 2% of the ABC).
b. Bank draft/guarantee or irrevocable letter of credit issued by a Universal bank: Provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a foreign bank (at least 2% of the ABC).
c. Surety bond, callable upon demand, issued by a surety or insurance company (at least 5% of the ABC) and a copy of certificate issued by the Insurance Commission certifying that the surety or insurance company is authorized to issue a surety bond.
d. Duly notarized Bid Securing Declaration (***Template per FORM 6***) **duly signed by the bidder’s authorized representative.**

<table>
<tr><th>Approved Budget for the Contract (ABC)</th><th>Cashier’s/manager’s check, Bank draft/guarantee or irrevocable letter of credit (2% of ABC)</th><th>Surety Bond (5% of ABC)</th><th>Bid Securing Declaration</th></tr>
<tr><td>**165,000,000.00**</td><td>**3,300,000.00**</td><td>**8,250,000.00**</td><td>**No required percentage**</td></tr>
</table>
</td></tr>
</table>

Item	**FIRST ENVELOPE: ELIGIBILITY DOCUMENTS AND TECHNICAL REQUIREMENTS (DULY SEALED AND MARKED)**
	The Bid Securing Declaration mentioned above is an undertaking which states, among others, that the bidder shall enter into contract with the Procuring Entity and furnish the performance security required under ITB Clause 31, within ten (10) calendar days from receipt of the Notice of Award, and commits to pay the corresponding amount as fine, and be suspended for a period of time from being qualified to participate in any government procurement activity in the event it violates any of the conditions stated therein as provided in the guidelines issued by the GPPB.
TAB 8	Accomplished Omnibus Sworn Statement (with ten [10] statements) (***Template per FORM 7***), **duly signed by the bidder's authorized representative and notarized.**
TAB 9	Accomplished Data Privacy Consent Form ***per FORM 8***, **duly signed by the bidder's authorized representative.**
TAB 10	Accomplished Certificate of Conformance to the Terms of Reference **per *FORM 9*, duly signed by the bidder's authorized representative.** The complete Terms of Reference and specifications are also attached as ***FORM 9-A*** for reference.
TAB 11	Accomplished Summary of Technical Compliance **per *Annex A of FORM 9-A*** for the proposed solution, ensuring it is cross-referenced with all of DBP's Terms of Reference, **duly signed by the bidder's authorized representative**
TAB 12	Certificate issued by the manufacturer/principal stating that the bidder is an authorized partner/reseller of the solutions being offered (up to 2nd tier). The certificate must clearly indicate the bidder's authority to distribute, implement, and support the solution products and services being offered.
TAB 13	Certificate issued in the name the bidder/principal for each of the following: i. ISO 27001 (Information Security Management Systems) ii. ISO 27014 (Governance and Information Security) iii. ISO 27034 (Application Security) iv. System and Organization Controls (SOC) 2 v. System and Organization Controls (SOC) 3 vi. Payment Card Industry Data Security Standard (PCI DSS)

Item	**SECOND ENVELOPE: FINANCIAL PROPOSAL (DULY SEALED AND MARKED)**
TAB 1	Duly accomplished Financial Proposal Form (***Template per FORM 10***), **duly signed by the bidder's authorized representative.** **Note: Bid shall not exceed the ABC of PhP 165,000,000.00 for 3 years or PhP 55,000,000.00 per year (inclusive of taxes.)**

TAB 2	Detailed Financial Proposal/Price Schedule duly signed by the bidder's authorized representative. Bidders shall use either **FORM 11-A or FORM 11-B** as template. **The total detailed bid must not exceed the ABC and must be consistent with the financial bid per TAB 1.**

IMPORTANT REMINDERS

A) Pursuant to Section 19.4 of the Instruction to Bidders, each and every page of the Bid Forms, under Section VI: Bidding Forms hereof, shall be signed by the duly authorized representative/s of the Bidder. Failure to do so shall be a ground for the rejection of the bid.

B) Any interlineations, erasures, or overwriting shall be valid only if they are signed or initialed by the duly authorized representative/s of the Bidder.

C) Bid documents shall be compiled in a folder/binder with the Annexes properly labeled with tabs/separators.

D) Bidders shall submit their bids through their duly authorized representative enclosed in separate sealed envelopes, which shall be submitted simultaneously:

a. The first sealed Envelope (1) shall contain the folder/binder of the Eligibility Requirements and Technical Component of the bid; prepared in three copies labeled as follows:
   - ORIGINAL – Eligibility Requirements and Technical Component
   - COPY1 – Eligibility Requirements and Technical Component
   - COPY2 – Eligibility Requirements and Technical Component

b. The next sealed Envelope (2) shall contain the folder/binder of the Financial Component of the bid; prepared in three copies labeled as follows:
   - ORIGINAL – Financial Component
   - COPY1 – Financial Component
   - COPY2 – Financial Component

c. Envelopes (1) and (2) shall then be enclosed in a single sealed, signed final/outer envelope/package/box.

d. All envelopes (Envelopes (1) to (2) and the final/outer envelope/package/box) shall indicate the following:
   - addressed to the Procuring Entity's BAC
   - name and address of the Bidder in capital letters
   - name of the contract/project to be bid in capital letters
   - bear the specific identification/reference code of this bidding process
   - bear a warning "DO NOT OPEN BEFORE…" the date and time for the opening of bids

E) Bids submitted after the deadline shall only be marked for recording purposes, shall not be included in the opening of bids, and shall be returned to the bidder unopened.

A. How to create and encrypt a password in an archived file

1. Launch the WinRAR application in your windows by clicking the windows button and type WinRAR at the search button. (Fig. 1.1) If you don’t have a WinRAR, download and install the program at www.win-rar.com (Fig. 1.2). For steps on how to download and install the WinRAR program, please refer to this link: https://www.wikihow.com/Use-WinRAR

   Avoid using the "Get WinRAR FREE with TrialPay" option. This will attempt to install adware on your computer.

   Fig. 1.1

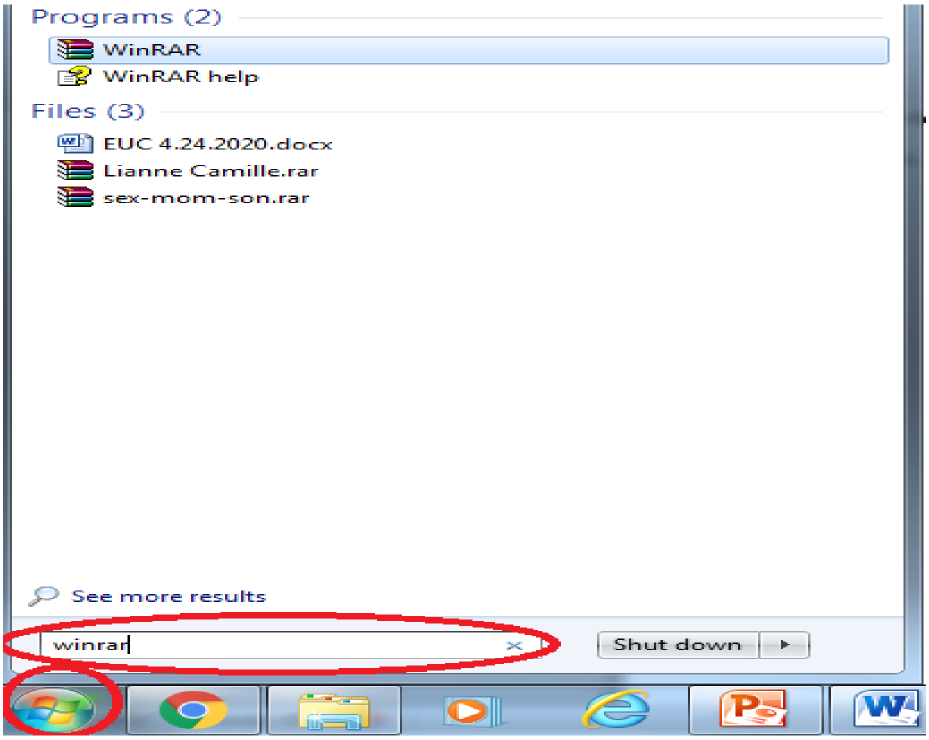
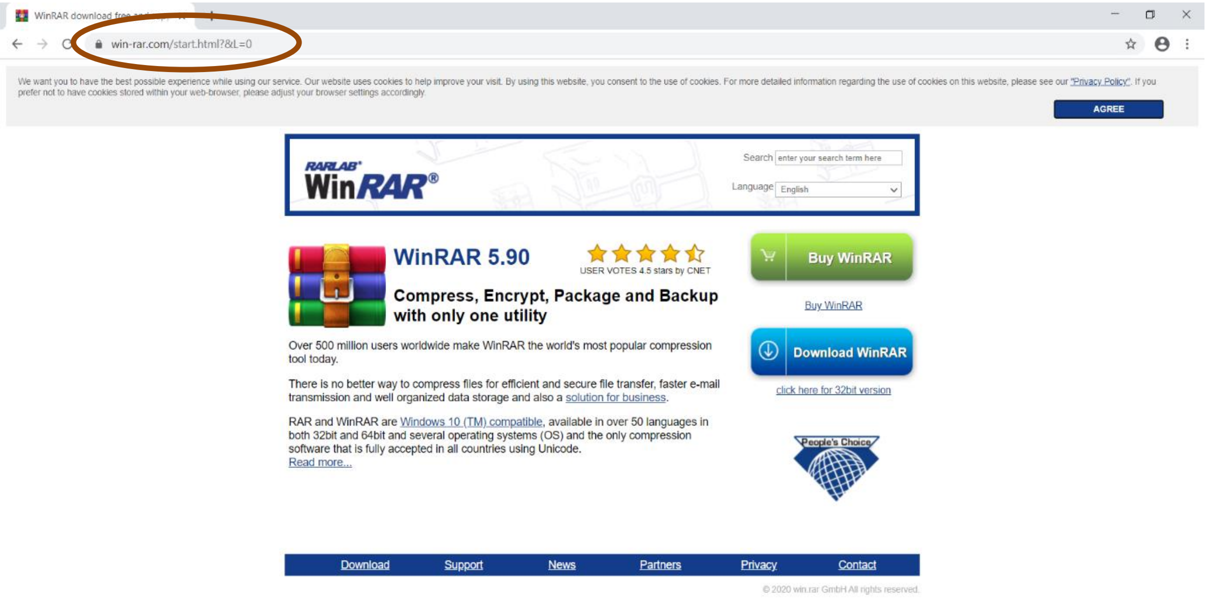


Fig. 1.2



We want you to have the best possible experience while using our service. Our website uses cookies to help improve your visit. By using this website, you consent to the use of cookies. For more detailed information regarding the use of cookies on this website, please see our "Privacy Policy". If you prefer not to have cookies stored within your web-browser, please adjust your browser settings accordingly.

WinRAR 5.90

USER VOTES 4.5 stars by CNET

Compress, Encrypt, Package and Backup with only one utility

Over 500 million users worldwide make WinRAR the world's most popular compression tool today.

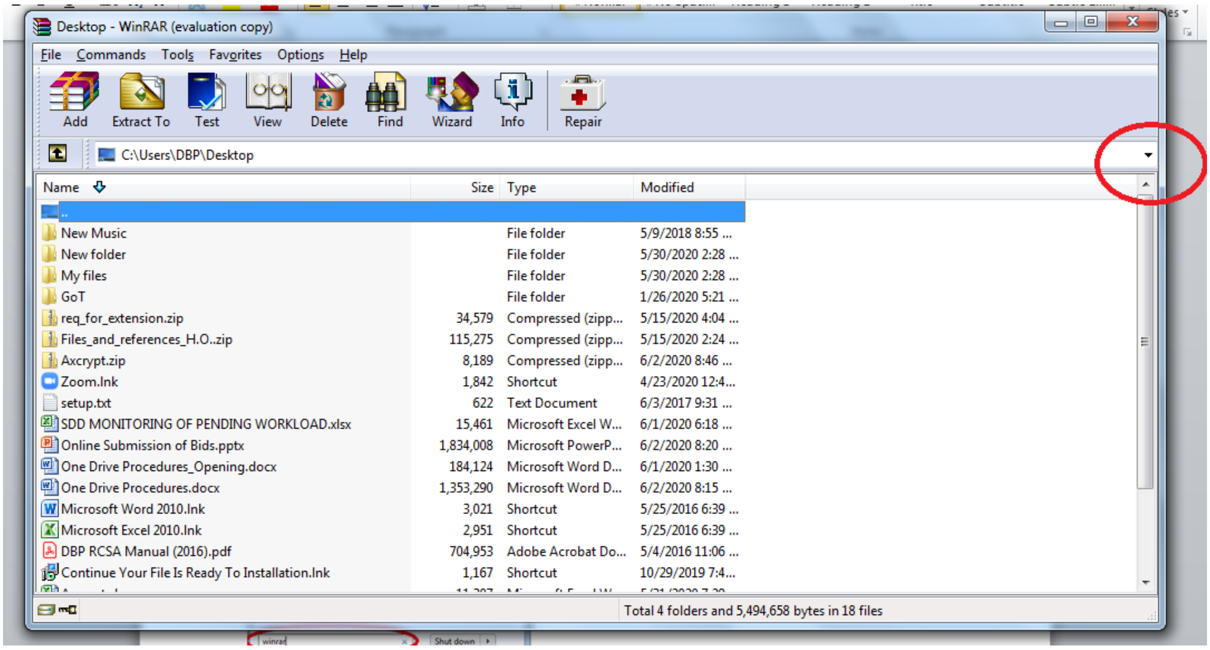
There is no better way to compress files for efficient and secure file transfer, faster e-mail transmission and well organized data storage and also a solution for business.

RAR and WinRAR are Windows 10 (TM) compatible, available in over 50 languages in both 32bit and 64bit and several operating systems (OS) and the only compression software that is fully accepted in all countries using Unicode.
Read more...

© 2020 win.rar GmbH All rights reserved.

2. Locate the file you want to zip by clicking the drop down menu. (Fig. 1.3)

Fig. 1.3

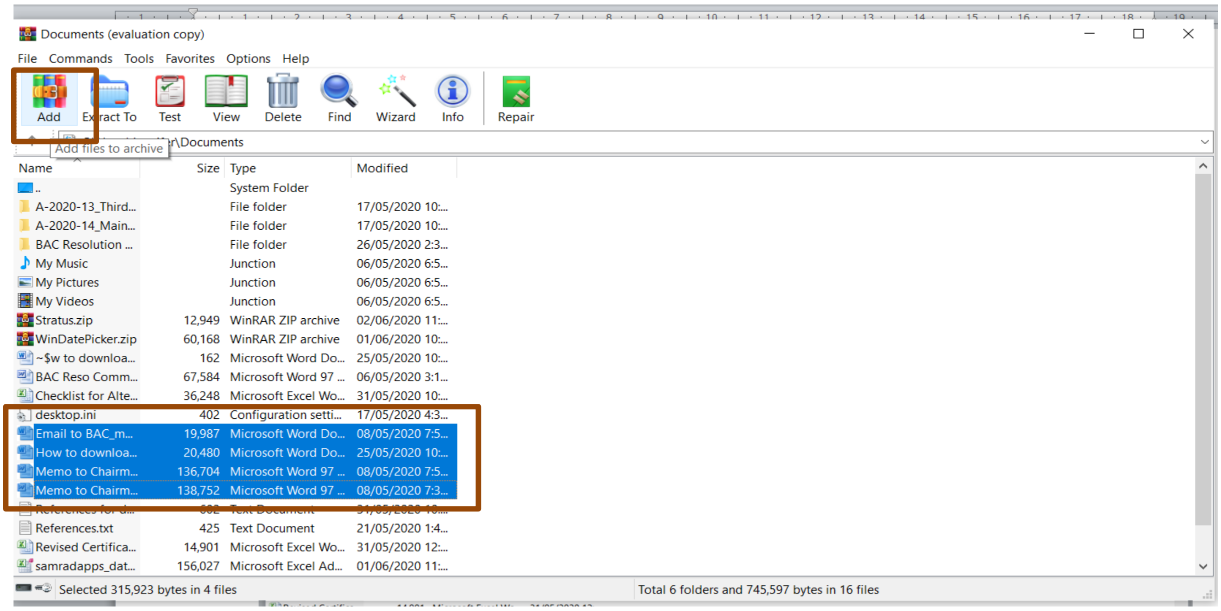


Name	Size	Type	Modified
..			
New Music		File folder	5/9/2018 8:55 ...
New folder		File folder	5/30/2020 2:28 ...
My files		File folder	5/30/2020 2:28 ...
GoT		File folder	1/26/2020 5:21 ...
req_for_extension.zip	34,579	Compressed (zipp...	5/15/2020 4:04 ...
Files_and_references_H.O..zip	115,275	Compressed (zipp...	5/15/2020 2:24 ...
Axcrypt.zip	8,189	Compressed (zipp...	6/2/2020 8:46 ...
Zoom.lnk	1,842	Shortcut	4/23/2020 12:4...
setup.txt	622	Text Document	6/3/2017 9:31 ...
SDD MONITORING OF PENDING WORKLOAD.xlsx	15,461	Microsoft Excel W...	6/1/2020 6:18 ...
Online Submission of Bids.pptx	1,834,008	Microsoft PowerP...	6/2/2020 8:20 ...
One Drive Procedures_Opening.docx	184,124	Microsoft Word D...	6/1/2020 1:30 ...
One Drive Procedures.docx	1,353,290	Microsoft Word D...	6/2/2020 8:15 ...
Microsoft Word 2010.lnk	3,021	Shortcut	5/25/2016 6:39 ...
Microsoft Excel 2010.lnk	2,951	Shortcut	5/25/2016 6:39 ...
DBP RCSA Manual (2016).pdf	704,953	Adobe Acrobat Do...	5/4/2016 11:06 ...
Continue Your File Is Ready To Installation.lnk	1,167	Shortcut	10/29/2019 7:4...

Total 4 folders and 5,494,658 bytes in 18 files

3. Select all of the files you want to archive in Windows by holding down the "Ctrl" key and left-click each file that you want to add to the archive. Add your files to a new RAR archive. There are a couple of different ways that you can do this:
   3.1 Open the WinRAR window and then browse for the files you want to add. Select all the files and then click the "Add" button; (Fig. 1.4) OR
   3.2 Select all of the files you want to archive in Windows. Right-click on your selection and choose "Add to archive..." (Fig. 1.5)

Fig. 1.4

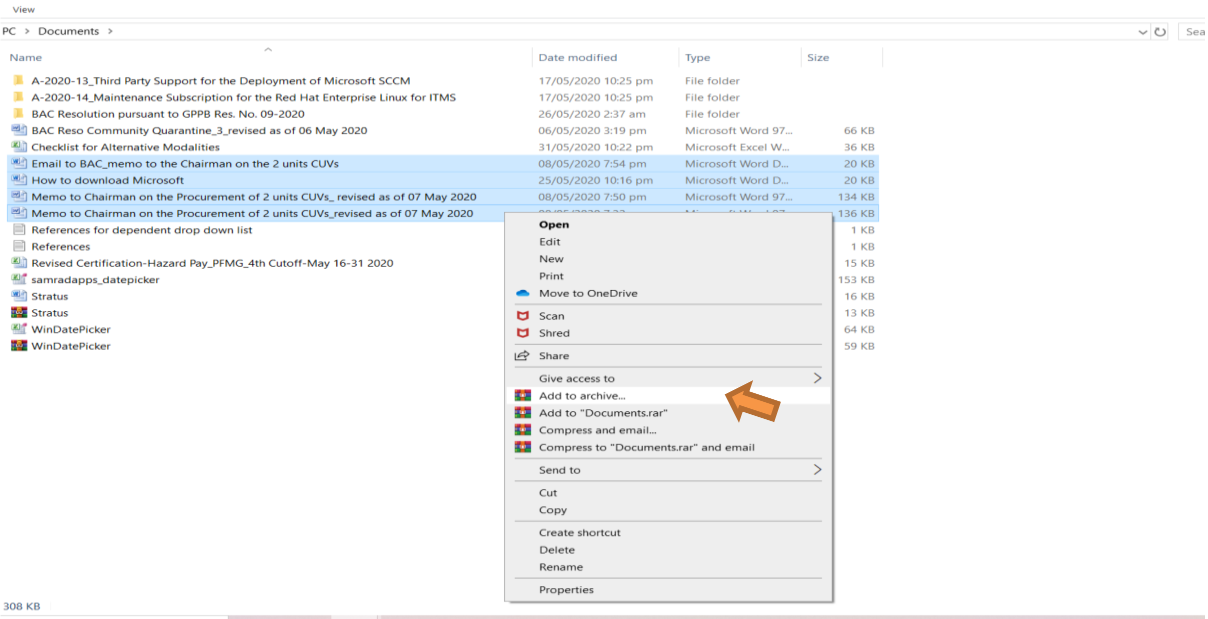


Name	Size	Type	Modified
..		System Folder	
A-2020-13_Third...		File folder	17/05/2020 10:...
A-2020-14_Main...		File folder	17/05/2020 10:...
BAC Resolution ...		File folder	26/05/2020 2:3...
My Music		Junction	06/05/2020 6:5...
My Pictures		Junction	06/05/2020 6:5...
My Videos		Junction	06/05/2020 6:5...
Stratus.zip	12,949	WinRAR ZIP archive	02/06/2020 11:...
WinDatePicker.zip	60,168	WinRAR ZIP archive	01/06/2020 10:...
~$w to downloa...	162	Microsoft Word Do...	25/05/2020 10:...
BAC Reso Comm...	67,584	Microsoft Word 97 ...	06/05/2020 3:1...
Checklist for Alte...	36,248	Microsoft Excel Wo...	31/05/2020 10:...
desktop.ini	402	Configuration setti...	17/05/2020 4:3...
Email to BAC_m...	19,987	Microsoft Word Do...	08/05/2020 7:5...
How to downloa...	20,480	Microsoft Word Do...	25/05/2020 10:...
Memo to Chairm...	136,704	Microsoft Word 97 ...	08/05/2020 7:5...
Memo to Chairm...	138,752	Microsoft Word 97 ...	08/05/2020 7:3...
References for d...	602	Text Document	31/05/2020 10:...
References.txt	425	Text Document	21/05/2020 1:4...
Revised Certifica...	14,901	Microsoft Excel Wo...	31/05/2020 12:...
samradapps_dat...	156,027	Microsoft Excel Ad...	01/06/2020 11:...

Selected 315,923 bytes in 4 files

Total 6 folders and 745,597 bytes in 16 files

Fig. 1.5

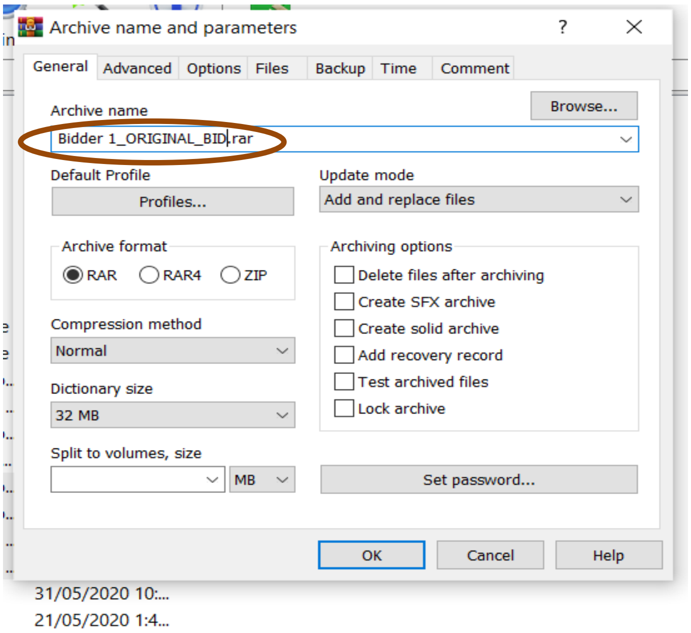


Name	Date modified	Type	Size
A-2020-13_Third Party Support for the Deployment of Microsoft SCCM	17/05/2020 10:25 pm	File folder	
A-2020-14_Maintenance Subscription for the Red Hat Enterprise Linux for ITMS	17/05/2020 10:25 pm	File folder	
BAC Resolution pursuant to GPPB Res. No. 09-2020	26/05/2020 2:37 am	File folder	
BAC Reso Community Quarantine_3_revised as of 06 May 2020	06/05/2020 3:19 pm	Microsoft Word 97...	66 KB
Checklist for Alternative Modalities	31/05/2020 10:22 pm	Microsoft Excel W...	36 KB
Email to BAC_memo to the Chairman on the 2 units CUVs	08/05/2020 7:54 pm	Microsoft Word D...	20 KB
How to download Microsoft	25/05/2020 10:16 pm	Microsoft Word D...	20 KB
Memo to Chairman on the Procurement of 2 units CUVs_ revised as of 07 May 2020	08/05/2020 7:50 pm	Microsoft Word 97...	134 KB
Memo to Chairman on the Procurement of 2 units CUVs_revised as of 07 May 2020			136 KB
References for dependent drop down list			1 KB
References			1 KB
Revised Certification-Hazard Pay_PFMG_4th Cutoff-May 16-31 2020			15 KB
samradapps_datepicker			153 KB
Stratus			16 KB
Stratus			13 KB
WinDatePicker			64 KB
WinDatePicker			59 KB

308 KB

4. Indicate your Archive name (e.g. Bidder 1_ORIGINAL_BID, Bidder 1_COPY NO. 1_BID, Bidder 1_COPY NO. 2_BID) (Fig. 1.6). By default, it will be named after the folder the files were originally in.

Fig. 1.6



Archive name and parameters

General | Advanced | Options | Files | Backup | Time | Comment

Archive name: Bidder 1_ORIGINAL_BID.rar

Default Profile: Profiles...

Update mode: Add and replace files

Archive format: ● RAR ○ RAR4 ○ ZIP

Compression method: Normal

Dictionary size: 32 MB

Split to volumes, size: MB

Archiving options
□ Delete files after archiving
□ Create SFX archive
□ Create solid archive
□ Add recovery record
□ Test archived files
□ Lock archive

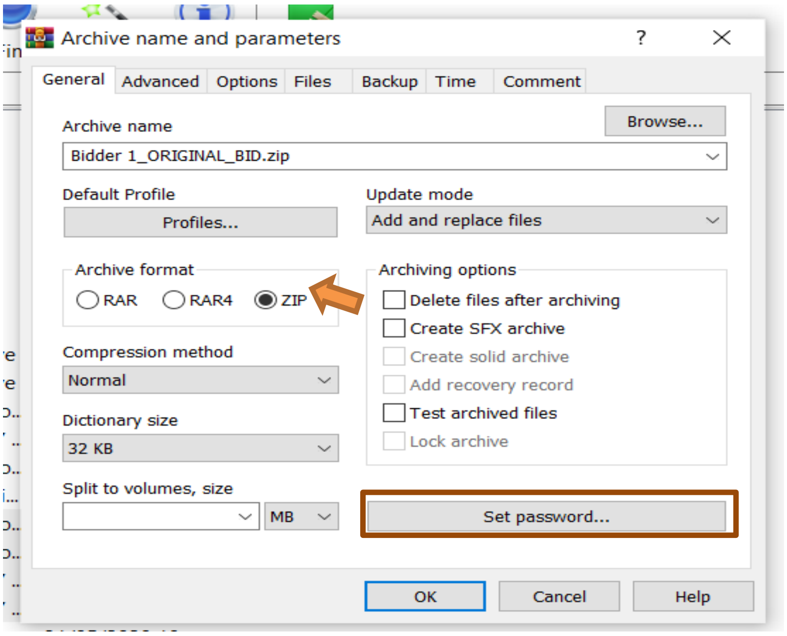
Set password...

OK | Cancel | Help

31/05/2020 10:...
21/05/2020 1:4...

5. Select the ◉ ZIP file button in the Archive format and then click the Set password… button. This is located in the General tab of the "Archive name and parameters" window that appears when creating a new archive. (Fig. 1.7)

Fig. 1.7



Archive name and parameters

General | Advanced | Options | Files | Backup | Time | Comment

Archive name: Bidder 1_ORIGINAL_BID.zip

Default Profile: Profiles...

Update mode: Add and replace files

Archive format: ○ RAR ○ RAR4 ● ZIP

Compression method: Normal

Dictionary size: 32 KB

Split to volumes, size: MB

Archiving options
□ Delete files after archiving
□ Create SFX archive
□ Create solid archive
□ Add recovery record
□ Test archived files
□ Lock archive

Set password...

OK | Cancel | Help

6. Type/Key in your password. (Fig. 1.8 and 1.9)

Fig. 1.8

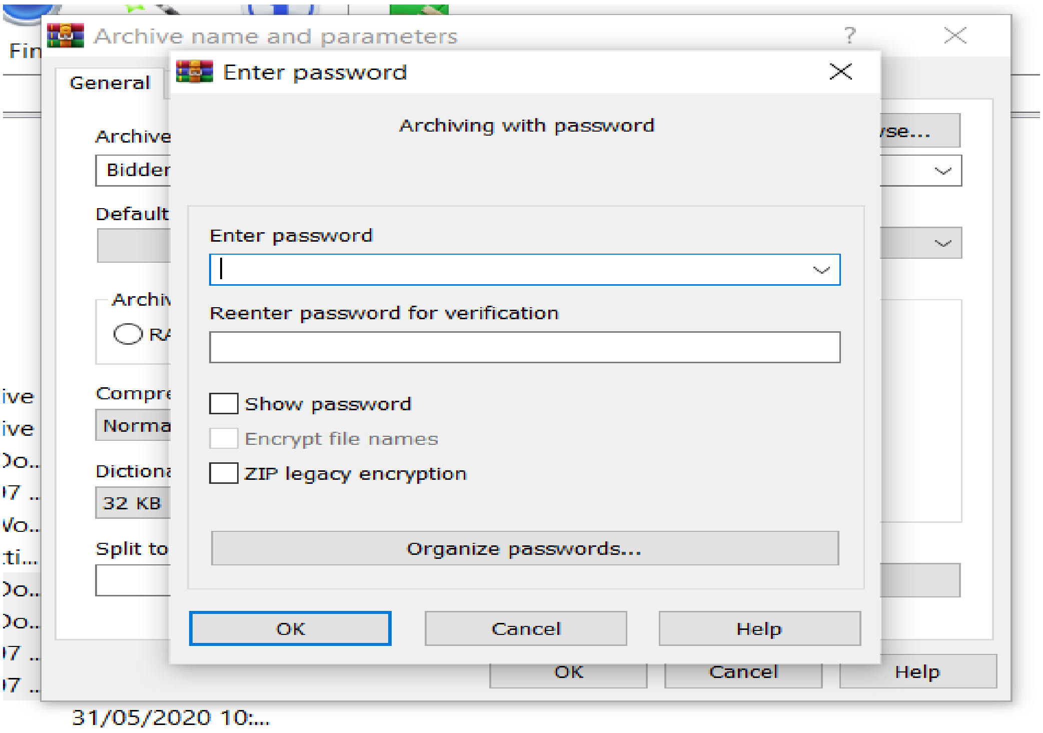
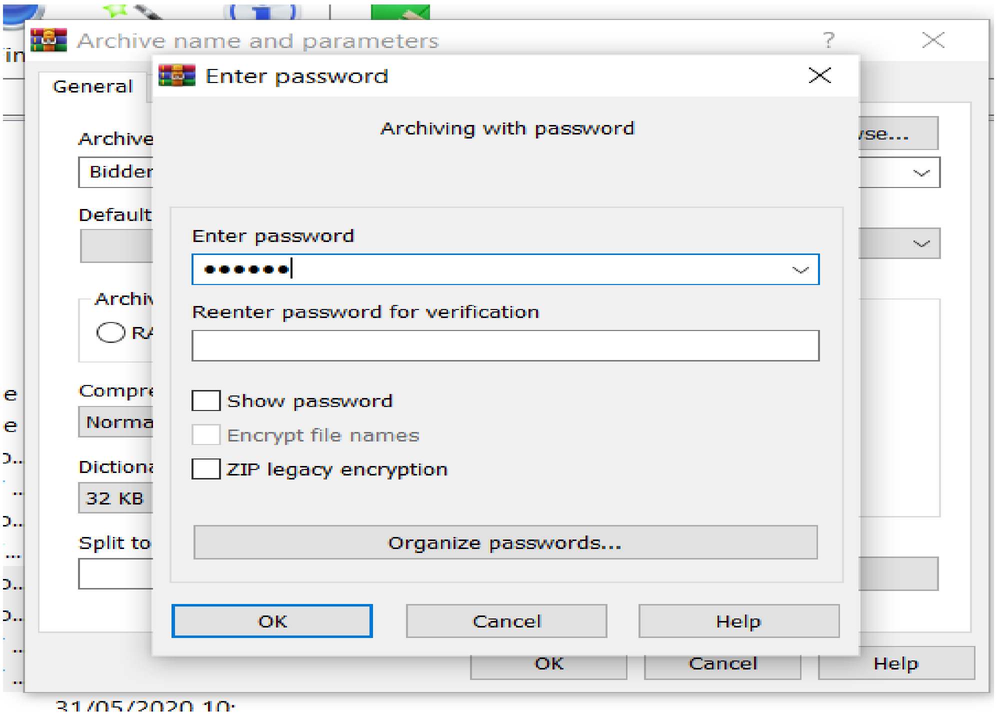
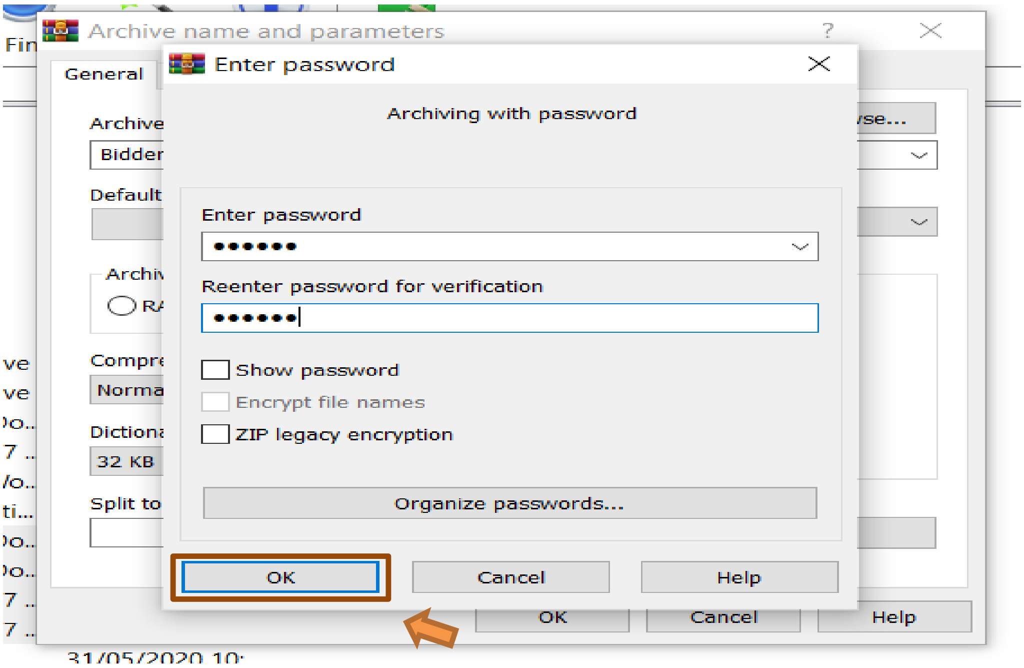


Fig. 1.9



7. Enter it a second time to confirm it. You can check the "Show password" box to see the characters as you type them (Fig. 1.10). After re-entering your password, click button to save your password.

Fig. 1.10


Enter password

Archiving with password

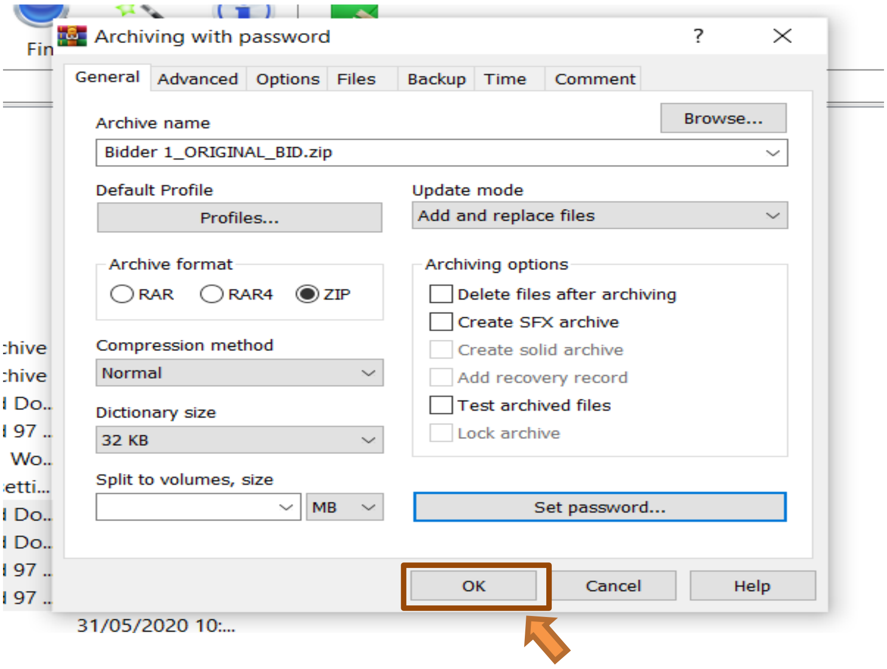
Enter password: ●●●●●●

Reenter password for verification: ●●●●●●

□ Show password
□ Encrypt file names
□ ZIP legacy encryption

8. After clicking OK in the “Enter password” tab, click OK in the "Archive with password" window to create your new .ZIP file. (Fig. 1.11)

Fig. 1.11


Archiving with password

General | Advanced | Options | Files | Backup | Time | Comment

Archive name: Bidder 1_ORIGINAL_BID.zip

Default Profile: Profiles...

Update mode: Add and replace files

Archive format: ○ RAR ○ RAR4 ● ZIP

Compression method: Normal

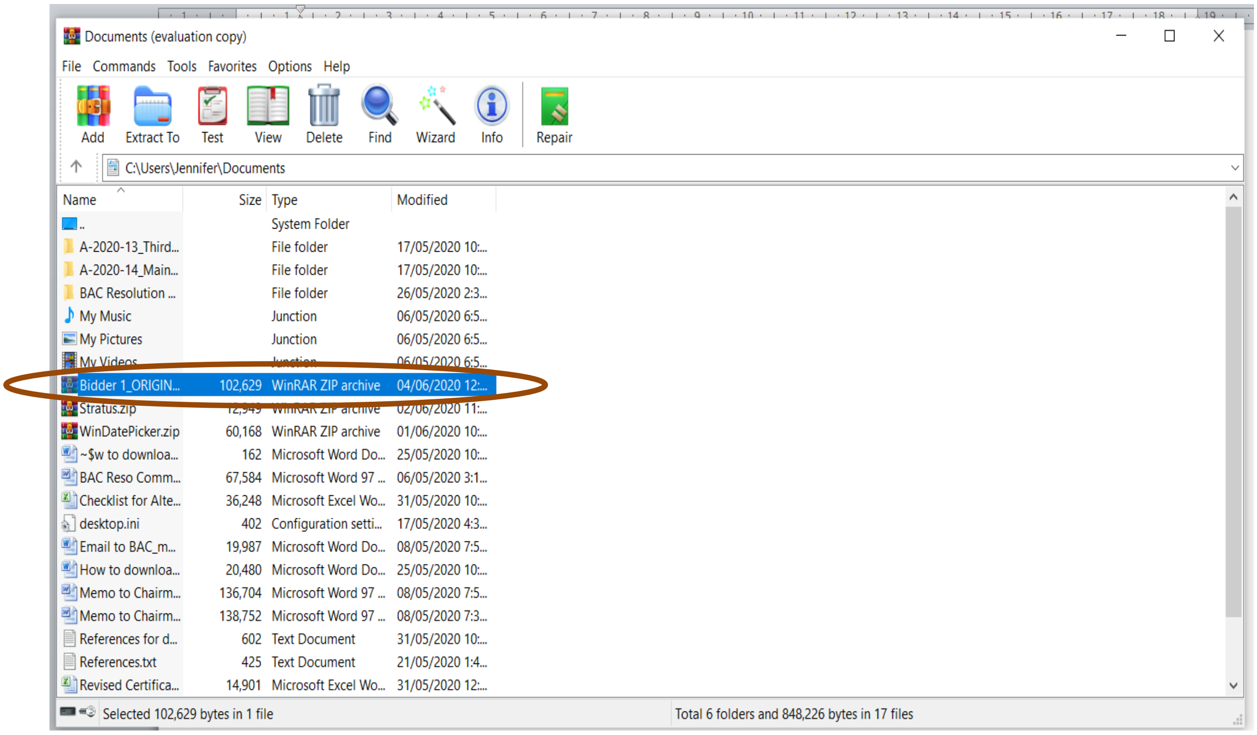
Dictionary size: 32 KB

Split to volumes, size: MB

Archiving options
□ Delete files after archiving
□ Create SFX archive
□ Create solid archive
□ Add recovery record
□ Test archived files
□ Lock archive

9. The program will show that the files you have already selected are already compressed. (Fig. 1.12)

Fig. 1.12


Documents (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
Repair

C:\Users\Jennifer\Documents

Name	Size	Type	Modified
..		System Folder	
A-2020-13_Third...		File folder	17/05/2020 10:...
A-2020-14_Main...		File folder	17/05/2020 10:...
BAC Resolution ...		File folder	26/05/2020 2:3...
My Music		Junction	06/05/2020 6:5...
My Pictures		Junction	06/05/2020 6:5...
My Videos		Junction	06/05/2020 6:5...
Bidder 1_ORIGIN...	102,629	WinRAR ZIP archive	04/06/2020 12:...
Stratus.zip	12,949	WinRAR ZIP archive	02/06/2020 11:...
WinDatePicker.zip	60,168	WinRAR ZIP archive	01/06/2020 10:...
~$w to downloa...	162	Microsoft Word Do...	25/05/2020 10:...
BAC Reso Comm...	67,584	Microsoft Word 97 ...	06/05/2020 3:1...
Checklist for Alte...	36,248	Microsoft Excel Wo...	31/05/2020 10:...
desktop.ini	402	Configuration setti...	17/05/2020 4:3...
Email to BAC_m...	19,987	Microsoft Word Do...	08/05/2020 7:5...
How to downloa...	20,480	Microsoft Word Do...	25/05/2020 10:...
Memo to Chairm...	136,704	Microsoft Word 97 ...	08/05/2020 7:5...
Memo to Chairm...	138,752	Microsoft Word 97 ...	08/05/2020 7:3...
References for d...	602	Text Document	31/05/2020 10:...
References.txt	425	Text Document	21/05/2020 1:4...
Revised Certifica...	14,901	Microsoft Excel Wo...	31/05/2020 12:...

Selected 102,629 bytes in 1 file

Total 6 folders and 848,226 bytes in 17 files

10. Test it out. After the .ZIP file is created, you can double-click it to test it out. When you try to extract it, you will be prompted for the password you created.

B. Procedures/steps for Online or Electronic Bid Submission:

I. All bidders who choose to submit their bids via our online bid submission facility shall properly notify the BAC Secretariat. The BAC Secretariat shall likewise provide assistance to the bidders on the procedures of online bid submission. Bidders shall be given the link as access to the online bid submission facility being used by the BAC.

1. The bidder shall send an email to the BAC Secretariat signifying its intent to submit their bids via DBP-BAC Online Bid Submission Facility. The bidder shall likewise request for the link of the Shared OneDrive Folder **(Microsoft Office 365 OneDrive)**.

2. The BAC Secretariat shall send the link of the Shared OneDrive Folder to the registered email being used by the bidder.

   Note: The email address being used by the bidder must be consistent or the same email address to be used by the BAC Secretariat in sending links of the Shared OneDrive Folder except for justifiable reasons (e.g., bidder is encountering technical issues or cannot access the link of the shared folder, etc.).
3. Once the bidder received the link of the Shared OneDrive Folder, he/she must notify the BAC Secretariat via email confirming receipt of the same link of the shared folder.

4. Upon gaining access or upon opening the Shared One Drive Folder, the bidder shall upload their bids, via proper labeling which is as follows:

   a. **(Name of Company/Office/Bidder)_FOLDER 1_ELIGIBILITY REQUIREMENTS AND TECHNICAL COMPONENT_BID**
   b. **(Name of Company/Office/Bidder)_FOLDER 2_FINANCIAL COMPONENT_BID**

   4.1 The bidder shall submit their bids **on or before the date and time of the Deadline for the Submission and Receipt of Bids as indicated in the Invitation to Bid (IB) par. 8.**

   4.2 The bidders are advised to take note of the schedule for the said activity at all times as indicated in the IB and the Bidding Documents and must check any Supplemental Bid Bulletins that will be issued/posted by the BAC from time to time which they can access and download for free in the PhilGEPS website and the DBP's website: https://www.dbp.ph/invitations-to-bid/

   4.3. Any revisions on the schedule of Deadline of the Submission and Receipt of Bids and the Opening of Bids shall be issued by the BAC and posted by the BAC Secretariat via a Supplemental Bid Bulletin and shall be used by the bidders as reference in submitting their bids.

5. Once the bidders have uploaded their bids, they shall properly notify the BAC Secretariat via email that their bids were successfully uploaded in the Shared OneDrive Folder.

6. The BAC Secretariat shall immediately notify the bidder or confirm via email that their bids were deemed uploaded and received by the BAC Secretariat and must indicate the exact date and time when the bids are received. The date and time of the receipt of the bid proposals shall be used by the BAC Secretariat during the Opening of Bids.

7. If the bidder desires to modify its bid, it shall likewise notify the BAC Secretariat of its intent to modify their bids.

   7.1 A bidder may modify its bid, ***provided:*** **that this is done before the deadline for the submission and receipt of bids.**

   7.2 If the bidder modifies its bid, it shall not be allowed to retrieve or delete its original electronically submitted bids but, shall only be allowed to send another bid equally labeled, properly identified, linked to its original electronically submitted bid and marked as a "modification".

   7.3 The BAC Secretariat shall equally notify the bidder on the date and time when the bid modifications were received via email.

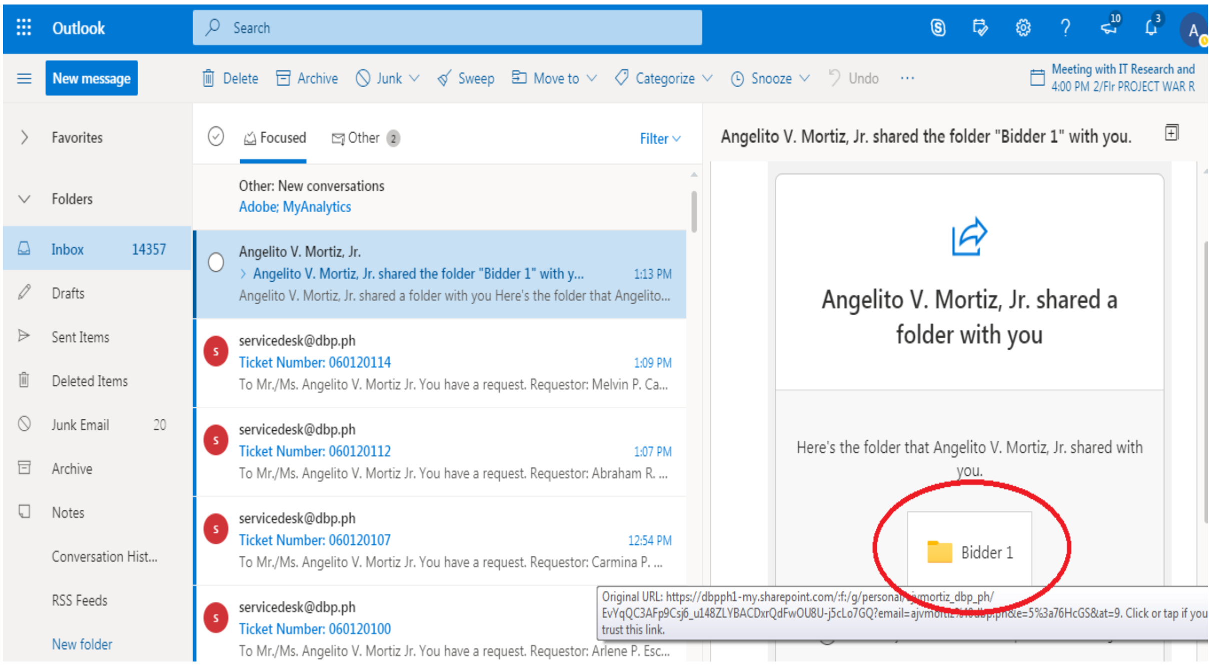
   7.4. Bid modifications received after the applicable deadline shall not be considered or rejected and shall not be opened during the Opening of Bids.

8. All bids received beyond the Deadline for the Submission and Receipt of Bids shall be automatically rejected.

C. How to Open the Link and Upload the Bid Proposals to the Shared OneDrive Folder

1. Open your email application and look for the email sending you the link for one drive and click the folder.

Fig. 1.1



Meeting with IT Research and 4:00 PM 2/Flr PROJECT WAR R

Other: New conversations
Adobe; MyAnalytics

Angelito V. Mortiz, Jr.
Angelito V. Mortiz, Jr. shared the folder "Bidder 1" with y... 1:13 PM
Angelito V. Mortiz, Jr. shared a folder with you Here's the folder that Angelito...

servicedesk@dbp.ph
Ticket Number: 060120114 1:09 PM
To Mr./Ms. Angelito V. Mortiz Jr. You have a request. Requestor: Melvin P. Ca...

servicedesk@dbp.ph
Ticket Number: 060120112 1:07 PM
To Mr./Ms. Angelito V. Mortiz Jr. You have a request. Requestor: Abraham R. ...

servicedesk@dbp.ph
Ticket Number: 060120107 12:54 PM
To Mr./Ms. Angelito V. Mortiz Jr. You have a request. Requestor: Carmina P. ...

servicedesk@dbp.ph
Ticket Number: 060120100
To Mr./Ms. Angelito V. Mortiz Jr. You have a request. Requestor: Arlene P. Esc...

Angelito V. Mortiz, Jr. shared the folder "Bidder 1" with you.

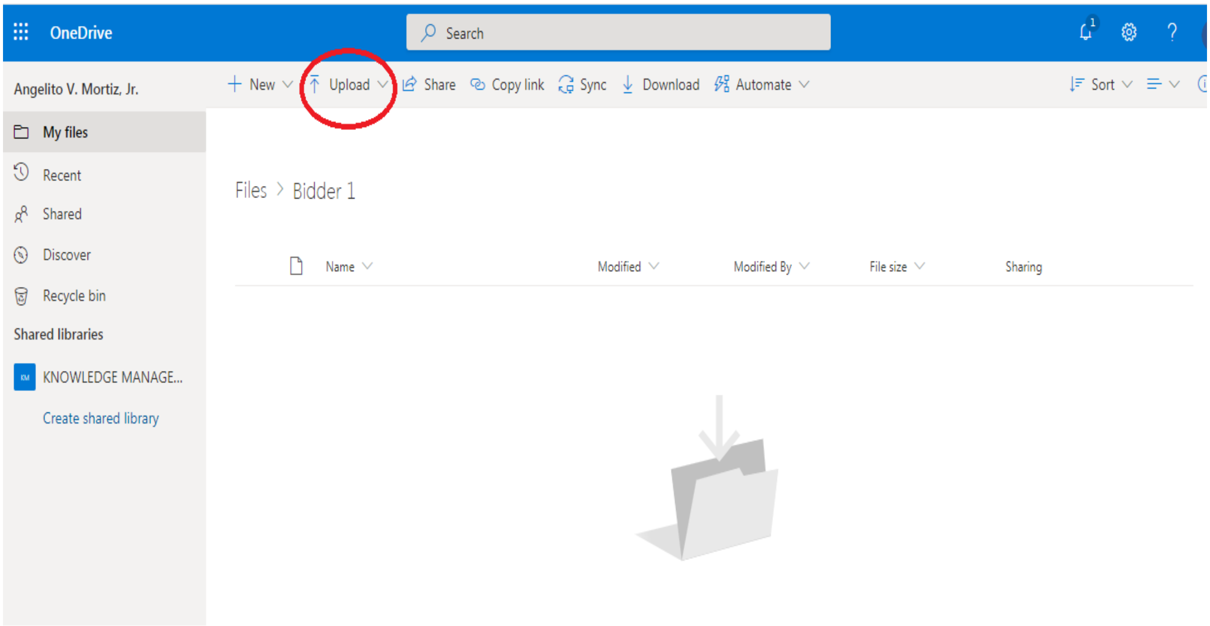
Angelito V. Mortiz, Jr. shared a folder with you

Here's the folder that Angelito V. Mortiz, Jr. shared with you.

Original URL: https://dbpph1-my.sharepoint.com/:f:/g/personal/ajvmortiz_dbp_ph/EvYqQC3AFp9Csj6_u148ZLYBACDxrQdFwOU8U-j5cLo7GQ?email=ajvmortiz%40dbp.ph&e=5%3a76HcGS&at=9. Click or tap if you trust this link.

2. Upon clicking the link, you will be directed to the One Drive folder. You may now upload the documents you wanted to share by clicking the upload button.

Fig. 2.1



Section IX: Bidding Forms

Bidding Forms

1ST ENVELOPE

Eligibility Documents

Technical Documents

2ND ENVELOPE

Financial Bid Form

FORM 1 (page 1 of 5)

PROTOCOL/UNDERTAKING TO ENTER INTO A JOINT VENTURE

KNOW ALL MEN BY THESE PRESENTS:

This Protocol/Undertaking to Enter into a Joint Venture "Undertaking" is made and executed by:

____________________________ (Name of the Bidder/Potential JV Partner), a sole proprietorship/partnership/corporation (Choose one, delete the others) duly organized and existing under Philippine laws, with principal office address at _____________________________ (Address), represented by its ________________ (Position of the Representative as indicated in the Secretary's Certificate), ______________________ (Name of the Authorized Representative as indicated in the Secretary's Certificate)

- and -

____________________________ (Name of the Bidder/Potential JV Partner), a sole proprietorship/partnership/corporation (Choose one, delete the others) duly organized and existing under Philippine laws, with principal office address at _____________________________ (Address), represented by its ________________ (Position of the Representative as indicated in the Secretary's Certificate), ______________________ (Name of the Authorized Representative as indicated in the Secretary's Certificate)

herein referred to collectively as the **"BIDDERS"**

- in favor of -

The **DEVELOPMENT BANK OF THE PHILIPPINES,** a financial institution created and operating pursuant to the provisions of Executive Order No. 81 dated December 3, 1986, otherwise known as the 1986 Revised Charter of the Development Bank of the Philippines, as amended by Republic Act No. 8523 dated February 14, 1998, with principal office at DBP Building, Sen. Gil J. Puyat Avenue, Makati City, Philippines, and herein referred to as **"DBP"** or the **"PROCURING ENTITY"**.

FORM 1 (page 2 of 5)

WITNESSETH:

WHEREAS, the **BIDDERS** desire to form and participate as a JOINT VENTURE ("JV") in the public bidding that will be conducted by the Development Bank of the Philippines pursuant to RA 9184 and its Revised IRR, with the following particulars:

Bid Reference No.:	
Name/Title of Procurement Project:	
Approved Budget for the Contract:	

WHEREAS, as of the date of submission of the bid for the above-mentioned procurement project of **DBP**, the **BIDDERS** have not executed or entered into a Joint Venture Agreement;

WHEREAS, pursuant to Sections 23.1(b) for Goods and 24.1(b) for Consulting Services of the 2016 Revised IRR of RA 9184, bidders that desire to participate in the bidding project as a Joint Venture, are required to submit a Joint Venture Agreement ("JVA") and in the absence thereof, a Notarized Statement from all the potential JV partners stating therein that they will enter into and abide by the provisions of the JVA in the event that the bid is successful and failure to enter into a joint venture within ten (10) calendar days after receipt of the Notice of Award shall be a ground for the forfeiture of the bid security;

NOW, THEREFORE, for and in consideration of the foregoing premises, the **BIDDERS**, hereby undertake in favor of the **PROCURING ENTITY**, as follows:

1. The **BIDDERS** shall enter into a JOINT VENTURE and sign and execute a Joint Venture Agreement and abide by its provisions in the event that the bid is successful in the above-mentioned procurement project of **DBP**.

2. The **BIDDERS** shall furnish **DBP**, through its Bids and Awards Committee (BAC) Secretariat, a duly signed and notarized copy of the JVA within ten (10) calendar days from receipt of the Notice from the DBP-BAC that the **BIDDERS** were declared as the Lowest Calculated and Responsive Bidder (LCRB) or Highest Rated and Responsive Bidder (HRRB), as the case may be.

3. For the purpose of executing and performing all acts necessary in order to participate in this bidding project, the following shall be the authorized representative of the **BIDDERS** or the JV to be formed as supported by the **BIDDER'S** respective Secretary's Certificate:[2]

[2] NAMES and ACTING AUTHORITY SHOULD CORRESPOND TO THAT STATED IN THE SUPPORTING SECRETARY'S CERTIFICATE FOR BOTH CORPORATIONS. EACH PARTNER'S SECRETARRY'S CERTICATE MUST STATE THE AUTHORIZED REPRESENTATIVE TO SIGN THE PROTOCOL TO FORM A JOINT VENTURE

FORM 1 (page 3 of 5)

Name	Company and Position	Specimen Signature
____________________	______________________	____________________
____________________	______________________	____________________
____________________	______________________	____________________

acting in this manner[3]:

1. □ Any one (1) of the above signatories
2. □ All of the above signatories
3. □ Any _(state the number)_ of the above signatories (in case the Board opts to have joint signing from designated representatives, i.e. any 2 jointly signing out of 3)

4. The **BIDDERS** shall indicate in the Joint Venture Agreement the following provisions, among others:

a. The JV Partners agree to be bound **jointly and severally** under the Joint Venture Agreement in relation to this bid project and the contract to be entered into with DBP;

b. The shareholdings and contribution of each JV Partner to the Joint Venture (with percentages [%]);

c. The Lead Partner Company of the JV is ______________________ ________________________ and the authorized representative of the JV from Lead Partner Company bidding is _________________________;

d. The Lead Company/JV Partner which shall be authorized to represent the JV in connection with this bid project specifying therein that the said lead company and the designated representative is duly authorized:

i) to execute the contract to be entered into by and between the JV and DBP **as indicated in Item No. 3 above**; and

ii) to issue the billing, sales invoice and receive any and all payments from DBP on behalf of the JV as well as the issuance of the corresponding official receipt.

e. The manner of management.

5. The **BIDDERS** further undertake that they shall comply with the 2016 IRR of RA 9184 or the Government Procurement Reform Act, and all other prevailing/applicable laws, as well as the policies of **DBP**.

6. The **BIDDERS** hereby acknowledge that pursuant to relevant provisions of the 2016 Revised IRR of RA 9184, failure on the part of the **BIDDERS** to enter into the Joint Venture, execute/sign a Joint Venture Agreement, and furnish DBP a notarized copy thereof within the period specified above after a Notice of Award was duly issued by **DBP,** for any reason, shall be a ground for non-issuance of the Notice to Proceed, forfeiture of the bid security and such other administrative and/or civil liabilities imposed under RA 9184 and its Revised IRR, GPPB Resolutions and Issuances, without liability on the part of **DBP**.

[3] Failure to indicate the manner of authority or to indicate the number in the third option shall mean that **ALL** authorized signatories **must sign** the bid documents.

FORM 1 (page 4 of 5)

7. The **BIDDERS** further acknowledge that in relation to this bidding project and Undertaking, notice to one of the **BIDDERS**/Potential JV Partners is deemed notice to all **BIDDERS**.

IN WITNESS WHEREOF, the **BIDDERS** have caused these presents to be signed at ____________(Place of Signing), Philippines this ________________ (Date of Signing).

BIDDERS:

______________________________	______________________________
(Name of JV Partner No. 1)	(Name of JV Partner No. 2)
By:	By:
______________________________	______________________________
(Name of the Authorized Signatory of JV Partner No. 1) (Position)	(Name of the Authorized Signatory of JV Partner No. 2) (Position)
Per Secretary's Certificate dated _______	Per Secretary's Certificate dated ______

FORM 1 (page 5 of 5)

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
MAKATI CITY) SS.

BEFORE ME, this ___ day of _________________ personally appeared:

Name	Competent Evidence of Identity	Place/Date Issued

known to me and to me known to be the same person/s who executed the foregoing instrument and who acknowledged to me that the same is his/her free and voluntary act and deed. This instrument, which consists of _______(__) pages, refers to a Protocol/Undertaking to Enter into a Joint Venture and signed by the Bidders and their instrumental witnesses on each and every page thereof.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed my notarial seal at the place and on the date first above written.

Doc. No. _______;
Page No. _______;
Book No. _______;
Series of 20__.

FORM 1-A (page 1 of 3)

For the Lead Partner of JV (Corporation)

REPUBLIC OF THE PHILIPPINES)
) SS.

SECRETARY'S CERTIFICATE

I, _________________________ (Name of the Corporate Secretary), the Corporate Secretary of the ____________________ (Name of the Corporation), a corporation duly organized and existing under and by virtue of the laws of the Philippines with principal office at __________________________________ (Address of the Corporation) **(the "Corporation")**, after having been duly sworn according to law, do hereby certify that at the meeting of the Board of Directors of the said Corporation duly convened and held on _______________ (Date of the meeting) at _____________________________ (Place of the meeting) at which a quorum was present and acted throughout, the following resolutions were unanimously approved and adopted through **Board Resolution No.** ___ (Indicate Board Resolution No.), **Series of 20__**:

> "**RESOLVED**, that the Corporation is hereby authorized to enter into a Joint Venter Agreement to participate in the bidding of ___________________ (Name of the Project and Project ID No.) of the Development Bank of the Philippines ("DBP" or the "Procuring Entity") as a Joint Venture ("JV") with ___________________ (Name of the Joint Venture Partner), hereinafter referred to as the "***JV***" pursuant to the terms and conditions of the Joint Venture Agreement ("JVA");
>
> **RESOLVED ALSO,** that in connection with the said bidding, the following is/are hereby appointed and designated as the duly authorized representative/s of the Corporation to the ***JV***, **to sign the Protocol/ Undertaking to Enter into A Joint Venture, the Joint Venture Agreement if Awarded the Contract, and to act as the Lead Partner of the said *JV***, granted with full power and authority to do, execute and perform any and all acts necessary for such purpose and/or to represent the Corporation to the ***JV*** in the bidding of the above-mentioned project, which includes to sign for and in behalf of the Corporation to the ***JV*** all bid and to sign contracts, agreements, instruments, statements, reports, and other documents pertaining to the bidding including the ensuing contract with DBP and all other documents, as may be required.

LEAD PARTNER: _______________ (NAME OF CORPORATION)

Name[4]	**Position**	**Specimen Signature**
____________________	____________________	____________________
____________________	____________________	____________________
____________________	____________________	____________________

[4] Both Corporations should designate the same representative/s to sign the bidding documents and the contract, if awarded the project subject of the bidding. The name must be consistent with the authorized representative as indicated in the Joint Venture Agreement.

acting in this manner[5]:

1. □ Any one (1) of the above signatories
2. □ All of the above signatories
3. □ Any _(state the number)___ of the above signatories (in case the Board opts to have joint signing from designated representatives, i.e. any 2 jointly signing out of 3)

RESOLVED FURTHER that, the _________________________ (Name of the Corporation):

(1) Submits itself to the jurisdiction of the Philippine government and waives its right to question the jurisdiction of the Philippine courts; and

(2) Shall neither seek nor obtain writs of injunction or prohibition or restraining order against the DBP or any other agency in connection with this project to prevent and restrain the bidding procedures related thereto, the negotiating of the award of a contract to a successful bidder, and the carrying out of the awarded contract.

RESOLVED FINALLY that, the foregoing authorities shall remain in full force and effect and binding on the Corporation until notice in writing is received by DBP, revoking, amending, or otherwise modifying the same."

The undersigned also certifies that _____________________ (Name of the Corporation's Signatory to the JVA) has been previously and duly authorized by the Board of the Directors thru Board Resolution No. ___, Series of ___ (Indicate the Board Resolution authorizing the Representative of the Corporation as Signatory to the JVA) to sign the JVA for and in behalf of the Corporation.

The undersigned further certifies that the foregoing resolutions have not been revoked, amended, or otherwise modified, and remain valid and subsisting.

The foregoing excerpts of the minutes of the Board meeting are true and correct and in accordance with the corporate records under my custody and are consistent with the Articles of Incorporation and By-laws of the Corporation.

IN WITNESS WHEREOF, I have hereunto affixed my signature on this ____ day of __________, 20__ at ______________.

____
Corporate Secretary

[5] Failure to indicate the manner of authority or to indicate the number in the third option shall mean that **ALL** authorized signatories **must sign** the bid documents.

FORM 1-A (page 3 of 3)

SUBSCRIBED AND SWORN to before me, this day of , 20__ at , affiant exhibiting to me his/her Competent Evidence of Identity issued on _______ at ______________.

NOTARY PUBLIC

Doc. No. _____________
Page No. _____________
Book No. _____________
Series of _____________

FORM 1-B (page 1 of 3)

For the Partner of JV (Corporation)

REPUBLIC OF THE PHILIPPINES)
) SS.

SECRETARY'S CERTIFICATE

I, _________________________ (Name of the Corporate Secretary), the Corporate Secretary of the ____________________ (Name of the Corporation), a corporation duly organized and existing under and by virtue of the laws of the Philippines with principal office at _________________________________ (Address of the Corporation) **(the "Corporation")**, after having been duly sworn according to law, do hereby certify that at the meeting of the Board of Directors of the said Corporation duly convened and held on _______________ (Date of the meeting) at _____________________________ (Place of the meeting) at which a quorum was present and acted throughout, the following resolutions were unanimously approved and adopted through **Board Resolution No.** ___ (Indicate Board Resolution No.)**, Series of 20**__:

"**RESOLVED**, that the Corporation is hereby authorized to enter into a Joint Venter Agreement to participate in the bidding of ___________________ (Name of the Project and Project ID No.) of the Development Bank of the Philippines ("DBP" or the "Procuring Entity") as a Joint Venture ("JV") with ___________________ (Name of the Joint Venture Partner), hereinafter referred to as the "***JV***" pursuant to the terms and conditions of the Joint Venture Agreement ("JVA");

RESOLVED ALSO, that in connection with the said bidding, the following is/are hereby appointed and designated as the duly authorized representative/s of the Corporation to the ***JV***, **to sign the Protocol/ Undertaking to Enter into A Joint Venture, the Joint Venture Agreement if Awarded the Contract, and to act as the Lead Partner of the said *JV***, granted with full power and authority to do, execute and perform any and all acts necessary for such purpose and/or to represent the Corporation to the ***JV*** in the bidding of the above-mentioned project, which includes to sign for and in behalf of the Corporation to the ***JV*** all bid and to sign contracts, agreements, instruments, statements, reports, and other documents pertaining to the bidding including the ensuing contract with DBP and all other documents, as may be required.

PARTNER: _______________ (NAME OF CORPORATION)

Name[6]	**Position**	**Specimen Signature**
____________________	____________________	____________________
____________________	____________________	____________________
____________________	____________________	____________________

[6] Both Corporations should designate the same representative/s to sign the bidding documents and the contract, if awarded the project subject of the bidding. The name must be consistent with the authorized representative as indicated in the Joint Venture Agreement.

acting in this manner[7]:

4. □ Any one (1) of the above signatories
5. □ All of the above signatories
6. □ Any _(state the number)___ of the above signatories (in case the Board opts to have joint signing from designated representatives, i.e. any 2 jointly signing out of 3)

RESOLVED FURTHER that, the ________________________ (Name of the Corporation):

(3) Submits itself to the jurisdiction of the Philippine government and waives its right to question the jurisdiction of the Philippine courts; and

(4) Shall neither seek nor obtain writs of injunction or prohibition or restraining order against the DBP or any other agency in connection with this project to prevent and restrain the bidding procedures related thereto, the negotiating of the award of a contract to a successful bidder, and the carrying out of the awarded contract.

RESOLVED FINALLY that, the foregoing authorities shall remain in full force and effect and binding on the Corporation until notice in writing is received by DBP, revoking, amending, or otherwise modifying the same."

The undersigned also certifies that ____________________ (Name of the Corporation's Signatory to the JVA) has been previously and duly authorized by the Board of the Directors thru Board Resolution No. ___, Series of ___ (Indicate the Board Resolution authorizing the Representative of the Corporation as Signatory to the JVA) to sign the JVA for and in behalf of the Corporation.

The undersigned further certifies that the foregoing resolutions have not been revoked, amended, or otherwise modified, and remain valid and subsisting.

The foregoing excerpts of the minutes of the Board meeting are true and correct and in accordance with the corporate records under my custody and are consistent with the Articles of Incorporation and By-laws of the Corporation.

IN WITNESS WHEREOF, I have hereunto affixed my signature on this ____ day of __________, 20__ at _____________.

____
Corporate Secretary

[7] Failure to indicate the manner of authority or to indicate the number in the third option shall mean that **ALL** authorized signatories **must sign** the bid documents.

FORM 1-B (page 3 of 3)

SUBSCRIBED AND SWORN to before me, this day of , 20__ at , affiant exhibiting to me his/her Competent Evidence of Identity issued on _______ at ______________.

NOTARY PUBLIC

Doc. No. _____________
Page No. _____________
Book No. _____________
Series of _____________

FORM 2-A (page 1 of 2)

(For Sole Proprietorships)

(use Bidder's Official Letterhead)

SPECIAL POWER OF ATTORNEY

I, ________________________, Filipino, of legal age, doing business under the trade name and style of "__________________", duly organized and existing under Philippine laws, with principal office address at __________________________ hereby name, constitute, and appoint ___________________________ (Name of Attorney-in-Fact) as my authorized representative and attorney-in-fact to do, execute, and perform any and all acts necessary to participate, submit bids, sign and execute documents and instruments, including the Bid Securing Declaration and/or to represent me in any and all bidding proceedings conducted by the Development Bank of the Philippines for the Bid Project ____________________________________ (Indicate Bid Project Title and No.):

I hereby grant, unto my said attorney-in-fact, full power and authority, to do, execute and perform all acts necessary or proper to render effective the power above-stated, as fully and effectively as I might or could lawfully do if personally present, and hereby ratifying and confirming all that my said attorney-in-fact shall do with full power of substitution and hereby further confirms all that said representative shall lawfully do or cause to be done by virtue hereof.

IN WITNESS WHEREOF, I have hereunto affixed my signature on this ____ day of ___________, 20__ at ______________.

____
Affiant/Principal

____
Attorney-in-Fact

Signed in the Presence of:

______________________ ____________________
Witness Witness

FORM 2-A (page 2 of 2)

(NOTE: PLS. USE THIS FORM **ONLY** IF THE REGISTERED PROPRIETOR OPTS TO AUTHORIZE ANOTHER PERSON TO REPRESENT HER/HIM TO DO, EXECUTE, AND PERFORM ANY AND ALL ACTS NECESSARY IN ORDER TO PARTICIPATE, SUBMIT BIDS, SIGN AND EXECUTE DOCUMENTS PERTAINING TO THE BID PROJECT.)

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
) SS.

BEFORE ME, a Notary Public for and in the (Province/City/Municipality) of _____________, personally appeared ___________________ with Identification No. _____________ issued on _____________ at _____________, known to me and to me known to be the same person who executed the foregoing instrument which he/she acknowledged to me to be his/her free and voluntary act and deed, consisting of only ______ (____) page/s, including this page in which this Acknowledgement is written, duly signed by him/her and his/her instrumental witnesses on each and every page hereof.

WITNESS MY HAND AND SEAL this _____________ at _____________, Philippines.

NOTARY PUBLIC

Doc. No. _____________
Page No. _____________
Book No. _____________
Series of _____________

FORM 2-B (page 1 of 3)

(For Corporations, Partnerships, or Cooperatives)

(use Bidder's Official Letterhead)

REPUBLIC OF THE PHILIPPINES)
) S.S.

SECRETARY'S CERTIFICATE

I, _________________________ (Name of the Corporate Secretary), the Corporate Secretary of the ____________________ (Name of the Corporation), a corporation duly organized and existing under and by virtue of the laws of the Philippines with principal office at _________________________________ (Address of the Corporation) (the "Corporation"), after having been duly sworn according to law, does hereby certify that at the meeting of the Board of Directors of the said Corporation duly convened and held on ______________ (Date of the meeting) at _____________________________ (Place of the meeting) at which a quorum was present and acted throughout, the following resolutions were unanimously approved and adopted through Board Resolution No. ___ (Indicate Board Resolution No.), Series of 20__:

> "**RESOLVED**, that the Corporation is hereby authorized to participate in the bidding of ___________________ (Name of the Project and Project ID No.) of the Development Bank of the Philippines ("DBP" or the "Procuring Entity") and if awarded the project shall enter into contract with DBP;
>
> **RESOLVED**, that in connection with the said bidding, the following is/are hereby appointed and designated as the duly authorized representative/s of the **Corporation**, granted with full power and authority to do, execute and perform any and all acts necessary and/or to represent the **Corporation** to participate in the bidding of the above-mentioned project which includes **to sign for and in behalf of the Corporation all bid documents, submit the bid**, and to sign contracts, agreements, instruments, statements, reports, and other documents pertaining to the bidding **including the ensuing contract with DBP** and all other documents, as may be required:

Name	**Position**	**Specimen Signature**
____________________	____________________	____________________
____________________	____________________	____________________
____________________	____________________	____________________

acting in this manner[8]:

1. □ Any one (1) of the above signatories
2. □ All of the above signatories
3. □ Any _(state the number)___ of the above signatories (in case the Board opts to have joint signing from designated representatives, i.e. any 2 jointly signing out of 3)

RESOLVED FURTHER THAT, the __________________ (Name of the Corporation):

(1) Submits itself to the jurisdiction of the Philippine government and waives its right to question the jurisdiction of the Philippine courts; and

(2) Shall neither seek nor obtain writs of injunction or prohibition or restraining order against the DBP or any other agency in connection with this project to prevent and restrain the bidding procedures related thereto, the negotiating of the award of a contract to a successful bidder, and the carrying out of the awarded contract.

RESOLVED FINALLY, that the foregoing authorities shall remain in full force and effect and binding on the Corporation until notice in writing is received by DBP, revoking, amending, or otherwise modifying the same."

The undersigned further certifies that the foregoing resolutions have not been revoked, amended, or otherwise modified, and remain valid and subsisting.

The foregoing excerpts of the minutes of the Board meeting are true and correct and in accordance with the corporate records under my custody and are consistent with the Articles of Incorporation and By-laws of the Corporation.

IN WITNESS WHEREOF, I have hereunto affixed my signature on this ____ day of __________, 20 at _____________.

____
Corporate Secretary

[8] Failure to indicate the manner of authority or to indicate the number in the third option shall mean that **ALL** authorized signatories **must sign** the bid documents.

FORM 2-B (page 3 of 3)

SUBSCRIBED AND SWORN to before me, this day of , 20 at , affiant exhibiting to me his/her Competent Evidence of Identity issued on _______ at ____________.

NOTARY PUBLIC

Doc. No. _____________
Page No. _____________
Book No. _____________
Series of _____________

FORM 3

(use Bidder's Official Letterhead)

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

STATEMENT OF ALL ONGOING GOVERNMENT & PRIVATE CONTRACTS INCLUDING CONTRACTS AWARDED BUT NOT YET STARTED (if any) (whether similar or not similar in nature)

Business Name : ______________________________

Business Address : ______________________________

Name of Contract/ Project Cost	*a) Client's Name* *b) Address* *c) Contact Person* *d) Contact Details (Telephone No. and Email Address)*	Nature of Work	*Bidder's Role*		*a) Date Awarded* *b) Date Started* c) Date of Completion	% of Accomplishment		Value of Outstanding Works / Undelivered Portion
			Description	%		*Planned*	*Actual*	
Government Contracts								
1)								
2)								
3)								
Private Contracts								
1)								
2)								
3)								

Submitted by : ______________________________
(Printed Name & Signature)

Designation : ______________________________

Date : ______________________________

FORM 4

(use Bidder's Official Letterhead)

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

STATEMENT OF SINGLE LARGEST CONTRACT (GOVERNMENT OR PRIVATE), OF SIMILAR NATURE COMPLETED WITHIN THE LAST FIVE (5) YEARS, EITHER:

Options	***SLCC Requirement***
1	**Single contract** equivalent to at least fifty percent (50%) of the ABC for one year; **OR**
2	**At least two (2) similar contracts**, the sum of which must be equivalent to at least fifty percent (50%) of the ABC for one year, provided the largest of these similar contracts must be at least twenty-five percent (25%) of the ABC for one year.

Business Name : ____________________

Business Address : ____________________

Name of Contract	*a) Client's Name* *b) Address* *c) Telephone number* *d) Email address*	Nature of Work	*Bidder's Role*		a) *Amount at Award* b) Amount at Completion c) Duration	a) Date Awarded b) Contract Effectivity c) Date Completed
			Description	%		

IMPORTANT: Please attach the following supporting documents related to each listed completed similar contract:

The identified single largest completed contracts must be supported by the following:

1) Notice of Award (NOA), **OR** Notice to Proceed (NTP), **OR** Contract/Purchase Order (PO)

AND

2) **Any one** of the following documents:
   2.1) Copy of Certificate of Completion or Certificate of Acceptance or Certificate of Satisfactory Performance issued by the bidder's client;

   2.2) Copy of Official Receipt/s or Sales Invoice/s issued by the bidder to the client (ORs/ SIs must sum up to the full amount of total contract price of completed project).

Submitted by : ____________________
(Printed Name & Signature)

Designation : ____________________

Date : ____________________

***Note: Similar contract shall refer to* any Cybersecurity Managed Services solutions which includes the delivery, subscription, installation, and/or maintenance and support**.

FORM 5

(use Bidder's Official Letterhead)

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

CERTIFICATE OF NET FINANCIAL CONTRACTING CAPACITY

The bidder must submit a computation of its Net Financial Contracting Capacity (NFCC), which must be at least equal to the ABC of the project to be bid, calculated as follows:

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

The value of the bidder's current assets and current liabilities shall be based on the Audited Financial Statement, stamped "RECEIVED" by the Bureau of Internal Revenue or BIR authorized collecting agent, for the immediately preceding year and a certified copy of Schedule of Fixed Assets particularly the list of construction equipment.

Current Assets (Year 20___)	
Minus: Current Liabilities (Year 20___)	
Sub-Total	
Multiplied by 15	
Sub-Total	
Minus: Value of Outstanding Contracts (per FORM 3)	
TOTAL	

Submitted by:

Name of Company/Bidder ______________________________
Name of Bidder's Authorized Representative ______________________________
Date ______________________________

Note: In case of Joint Venture, the partner responsible to submit the NFCC shall likewise submit the Statement of all its ongoing contracts and the latest EFPS Filed Audited Financial Statements

FORM 6 (page 1 of 2)

Bid Securing Declaration Form
[shall be submitted with the Bid if bidder opts to provide this form of bid security]

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

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.

FORM 6 (page 2 of 2)

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

SUBSCRIBED AND SWORN to before me this __ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her *[insert type of government identification card used]*, with his/her photograph and signature appearing thereon.

Witness my hand and seal this ___ day of *[month] [year].*

NAME OF NOTARY PUBLIC
Serial No. of Commission ______________
Notary Public for __________ until ________
Roll of Attorneys No.__________________
PTR No.______, *[date issued], [place issued]*
IBP No.______, *[date issued], [place issued]*

Doc. No. __________
Page No. __________
Book No. __________
Series of __________

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

OMNIBUS SWORN STATEMENT

[shall be submitted with the Bid]

____

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;**

<u>FORM 7 (page 2 of 3)</u>

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.

FORM 7 (page 3 of 3)

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

SUBSCRIBED AND SWORN to before me this __ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her *[insert type of government identification card used]*, with his/her photograph and signature appearing thereon.

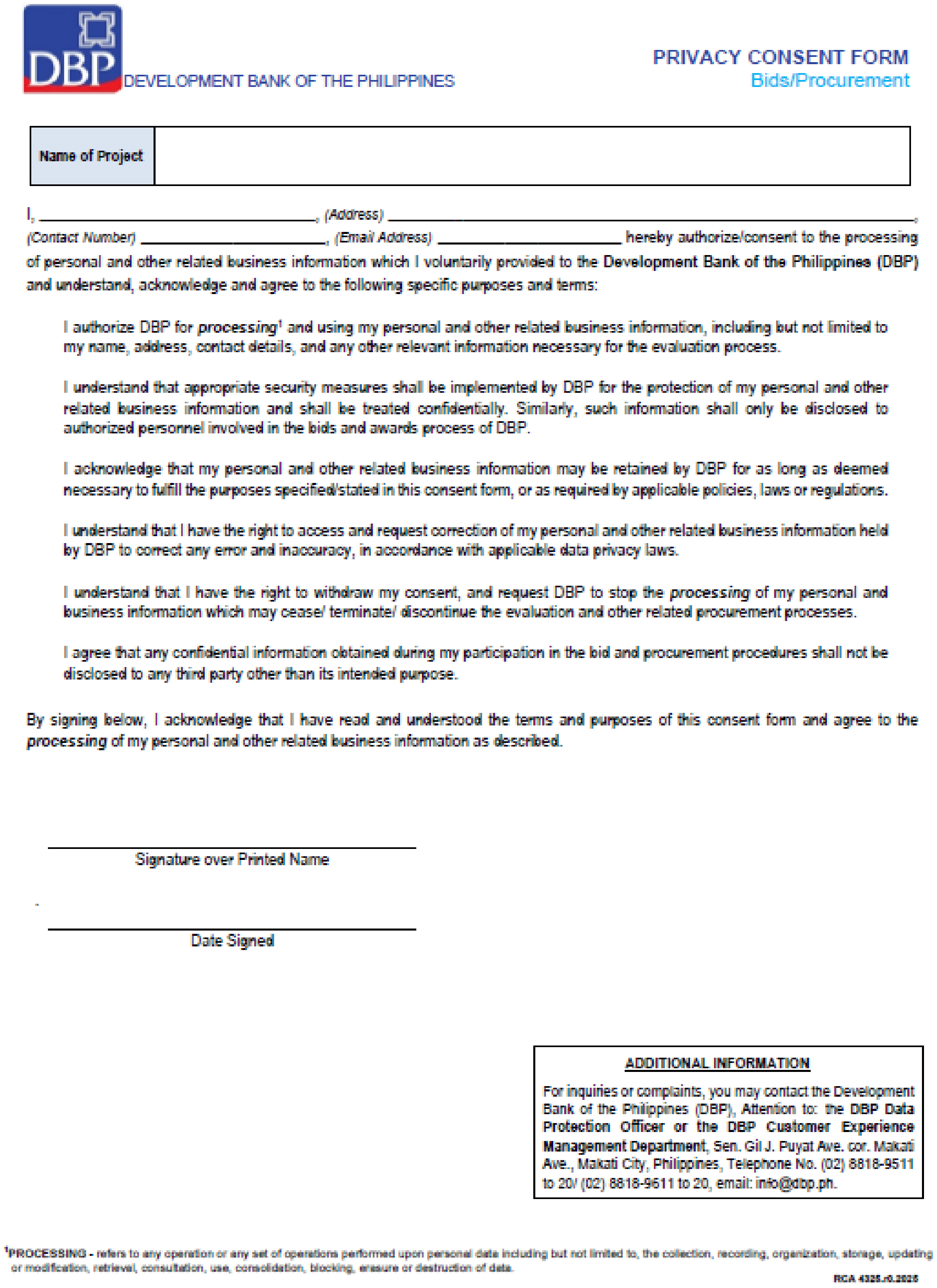
Witness my hand and seal this ___ day of *[month] [year].*

NAME OF NOTARY PUBLIC
Serial No. of Commission ______________
Notary Public for _________ until _______
Roll of Attorneys No.__________________
PTR No._____, *[date issued], [place issued]*
IBP No._____, *[date issued], [place issued]*

Doc. No. __________
Page No. __________
Book No. __________
Series of __________

FORM 8

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20



DBP DEVELOPMENT BANK OF THE PHILIPPINES

PRIVACY CONSENT FORM
Bids/Procurement

Name of Project	

I, ______________________________, *(Address)* ____,
(Contact Number) ____________________, *(Email Address)* ____________________ hereby authorize/consent to the processing of personal and other related business information which I voluntarily provided to the **Development Bank of the Philippines (DBP)** and understand, acknowledge and agree to the following specific purposes and terms:

I authorize DBP for *processing*[1] and using my personal and other related business information, including but not limited to my name, address, contact details, and any other relevant information necessary for the evaluation process.

I understand that appropriate security measures shall be implemented by DBP for the protection of my personal and other related business information and shall be treated confidentially. Similarly, such information shall only be disclosed to authorized personnel involved in the bids and awards process of DBP.

I acknowledge that my personal and other related business information may be retained by DBP for as long as deemed necessary to fulfill the purposes specified/stated in this consent form, or as required by applicable policies, laws or regulations.

I understand that I have the right to access and request correction of my personal and other related business information held by DBP to correct any error and inaccuracy, in accordance with applicable data privacy laws.

I understand that I have the right to withdraw my consent, and request DBP to stop the *processing* of my personal and business information which may cease/ terminate/ discontinue the evaluation and other related procurement processes.

I agree that any confidential information obtained during my participation in the bid and procurement procedures shall not be disclosed to any third party other than its intended purpose.

By signing below, I acknowledge that I have read and understood the terms and purposes of this consent form and agree to the *processing* of my personal and other related business information as described.

____
Signature over Printed Name

____
Date Signed

ADDITIONAL INFORMATION

For inquiries or complaints, you may contact the Development Bank of the Philippines (DBP), Attention to: the **DBP Data Protection Officer or the DBP Customer Experience Management Department**, Sen. Gil J. Puyat Ave. cor. Makati Ave., Makati City, Philippines, Telephone No. (02) 8818-9511 to 20/ (02) 8818-9611 to 20, email: info@dbp.ph.

[1] **PROCESSING -** refers to any operation or any set of operations performed upon personal data including but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

RCA 4325.r0.2025

FORM 9

(use Bidder's Official Letterhead)

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

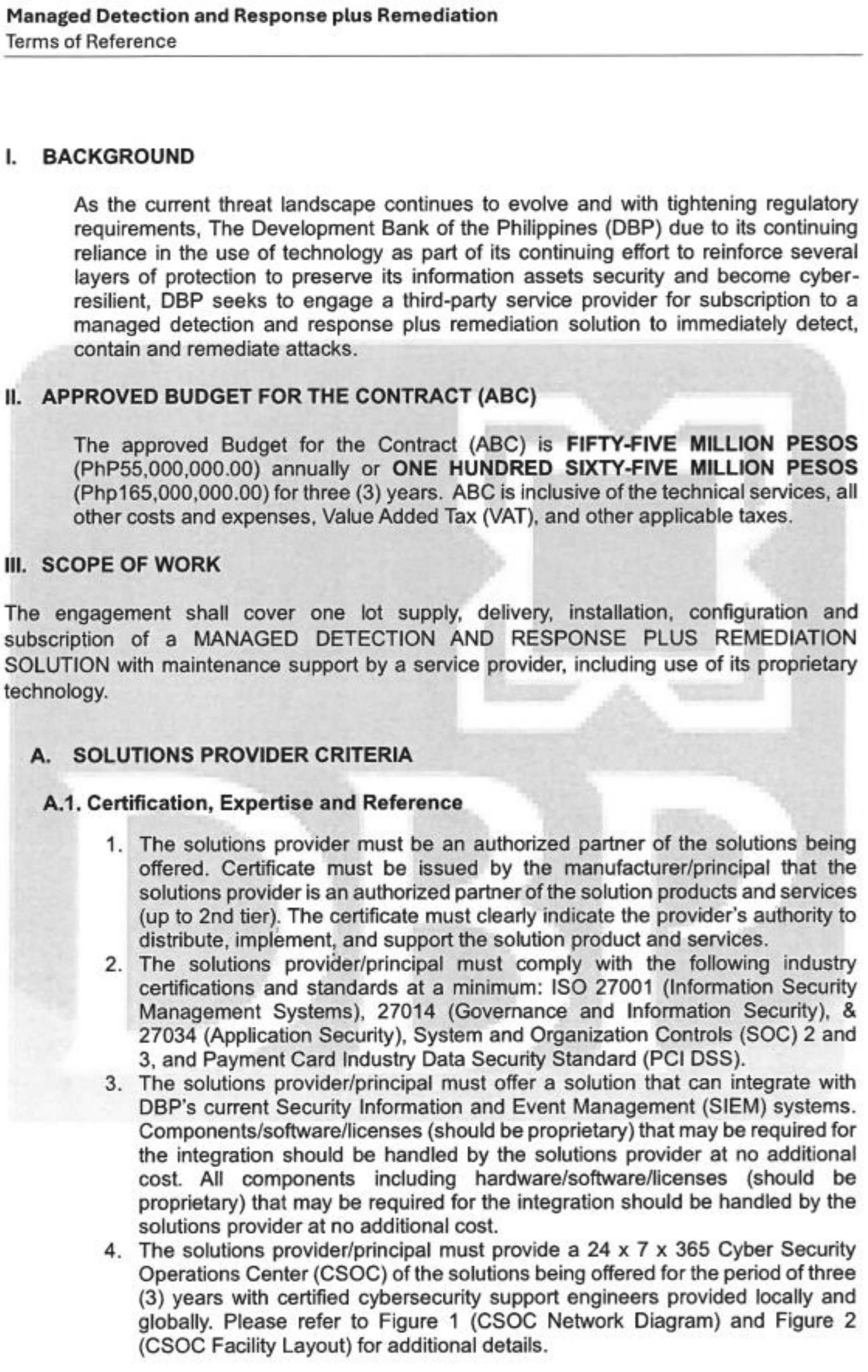
CERTIFICATE OF CONFORMANCE TO THE TERMS OF REFERENCE AND SPECIFICATIONS

I/we, ______________________________ the authorized representative/s of ____________*(name of company)*____________, hereby certify the following:

- That we have thoroughly read and understood the complete set of the bidding documents for the project, particularly the Scope of Works/Terms of Reference, its specifications and requirements, including all revisions, amendments, and supplemental bulletins.

- That should we be awarded the contract, we shall conform and comply to all specifications and requirements as specified in the project's bidding documents and its Terms and Reference.

______________________________ *Name and Signature of Representative*	______________________________ *Name of Company (Bidder)*
______________________________ *Position*	______________________________ *Address*
______________________________ *Contact Numbers*	______________________________ *Date Signed*



I. BACKGROUND

As the current threat landscape continues to evolve and with tightening regulatory requirements, The Development Bank of the Philippines (DBP) due to its continuing reliance in the use of technology as part of its continuing effort to reinforce several layers of protection to preserve its information assets security and become cyber-resilient, DBP seeks to engage a third-party service provider for subscription to a managed detection and response plus remediation solution to immediately detect, contain and remediate attacks.

II. APPROVED BUDGET FOR THE CONTRACT (ABC)

The approved Budget for the Contract (ABC) is **FIFTY-FIVE MILLION PESOS** (PhP55,000,000.00) annually or **ONE HUNDRED SIXTY-FIVE MILLION PESOS** (Php165,000,000.00) for three (3) years. ABC is inclusive of the technical services, all other costs and expenses, Value Added Tax (VAT), and other applicable taxes.

III. SCOPE OF WORK

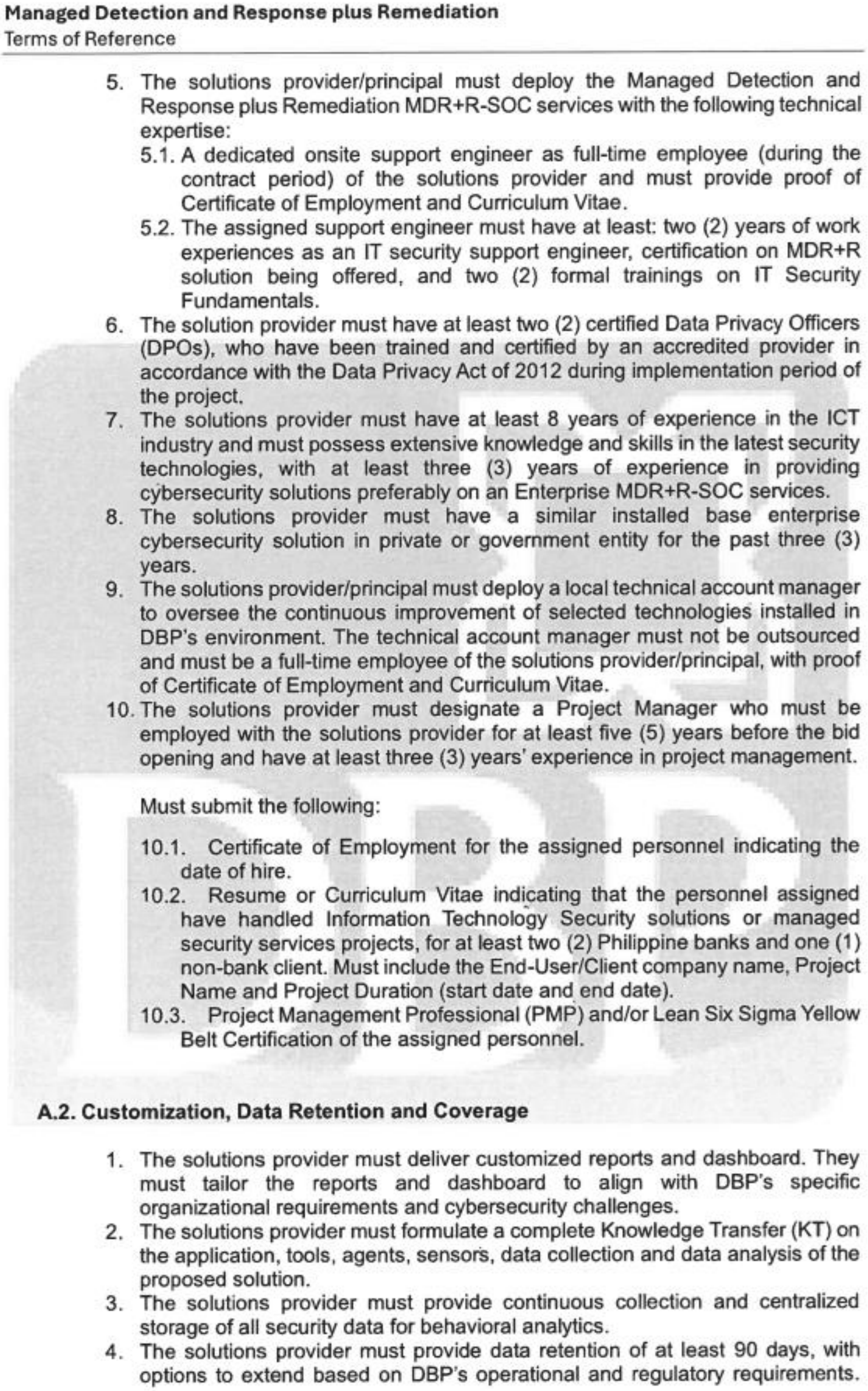
The engagement shall cover one lot supply, delivery, installation, configuration and subscription of a MANAGED DETECTION AND RESPONSE PLUS REMEDIATION SOLUTION with maintenance support by a service provider, including use of its proprietary technology.

A. SOLUTIONS PROVIDER CRITERIA

A.1. Certification, Expertise and Reference

1. The solutions provider must be an authorized partner of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.
2. The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).
3. The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.
4. The solutions provider/principal must provide a 24 x 7 x 365 Cyber Security Operations Center (CSOC) of the solutions being offered for the period of three (3) years with certified cybersecurity support engineers provided locally and globally. Please refer to Figure 1 (CSOC Network Diagram) and Figure 2 (CSOC Facility Layout) for additional details.

FORM 9-A (page 2 of 29)



5. The solutions provider/principal must deploy the Managed Detection and Response plus Remediation MDR+R-SOC services with the following technical expertise:
   5.1. A dedicated onsite support engineer as full-time employee (during the contract period) of the solutions provider and must provide proof of Certificate of Employment and Curriculum Vitae.
   5.2. The assigned support engineer must have at least: two (2) years of work experiences as an IT security support engineer, certification on MDR+R solution being offered, and two (2) formal trainings on IT Security Fundamentals.
6. The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.
7. The solutions provider must have at least 8 years of experience in the ICT industry and must possess extensive knowledge and skills in the latest security technologies, with at least three (3) years of experience in providing cybersecurity solutions preferably on an Enterprise MDR+R-SOC services.
8. The solutions provider must have a similar installed base enterprise cybersecurity solution in private or government entity for the past three (3) years.
9. The solutions provider/principal must deploy a local technical account manager to oversee the continuous improvement of selected technologies installed in DBP's environment. The technical account manager must not be outsourced and must be a full-time employee of the solutions provider/principal, with proof of Certificate of Employment and Curriculum Vitae.
10. The solutions provider must designate a Project Manager who must be employed with the solutions provider for at least five (5) years before the bid opening and have at least three (3) years' experience in project management.

    Must submit the following:

    10.1. Certificate of Employment for the assigned personnel indicating the date of hire.
    10.2. Resume or Curriculum Vitae indicating that the personnel assigned have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date).
    10.3. Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.

A.2. Customization, Data Retention and Coverage

1. The solutions provider must deliver customized reports and dashboard. They must tailor the reports and dashboard to align with DBP's specific organizational requirements and cybersecurity challenges.
2. The solutions provider must formulate a complete Knowledge Transfer (KT) on the application, tools, agents, sensors, data collection and data analysis of the proposed solution.
3. The solutions provider must provide continuous collection and centralized storage of all security data for behavioral analytics.
4. The solutions provider must provide data retention of at least 90 days, with options to extend based on DBP's operational and regulatory requirements.

Compliance with industry standards and legal mandates for data storage and privacy.

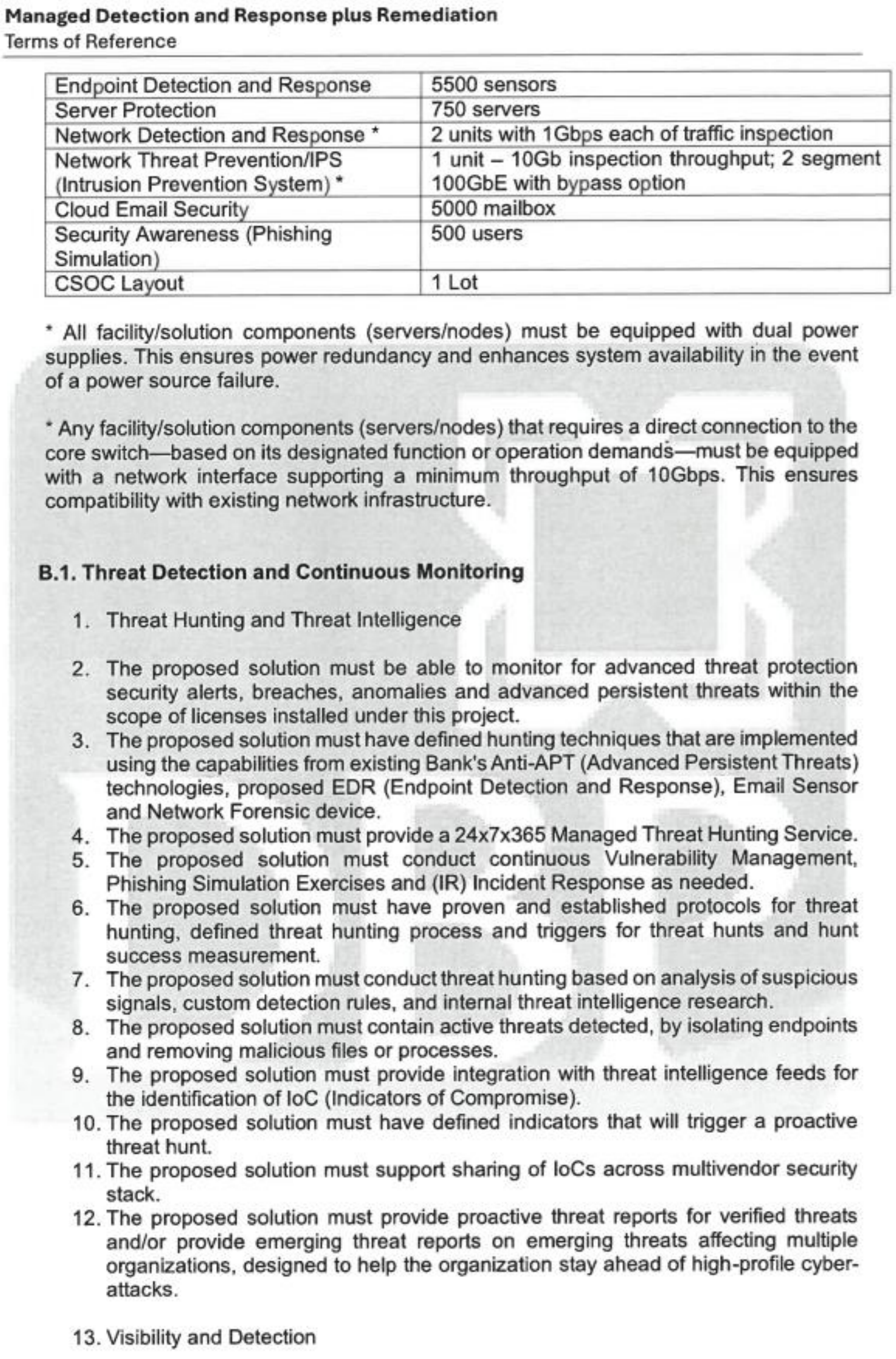
5. The solutions provider must provide a visibility of lateral movement across the network and other parts of the infrastructure
6. The solutions provider must support detection and response for threats involving managed and unmanaged endpoints, servers, networks, managed email users/mailbox and remote users. Detection mechanisms must include signature-based, behavioral, and AI-driven techniques, with automated response workflows and alerting.

A.3. Trainings, Security Awareness and Other Requirements

1. The solutions provider must formulate a comprehensive cybersecurity training program with TESDA-accredited training center for the following modules and participants:
   1.1. Basic Administration for at least ten (10) participants
   1.2. Knowledge Transfer (Minimum of One (1) knowledge transfer session provided onsite with complete materials.)
2. The solutions provider must develop an Annual Security Posture Assessment Plan, which includes a comprehensive evaluation of DBP's security measures and recommendations for enhancements.
3. The solutions provider must conduct phishing simulation with a unified platform that allows DBP to perform unlimited phishing simulation exercises and security awareness trainings.
4. The solutions provider must include Security Awareness licenses for at least 500 users per campaign and allow tracking of campaigns.
5. The solutions provider must provide phishing simulation tool with standard templates and allow creation of custom templates. The phishing simulation tool must allow recipients to be chosen from different data sources such as but not limited to Active directory, Microsoft Entra ID and Okta.
6. The solutions provider must provide phishing simulation tool with training campaigns. The training campaigns must have training programs in video and interactive format and be targeted for a list of recipients. The training programs must include the following training categories:
   6.1. Business Email Compromise
   6.2. Executives
   6.3. Malware
   6.4. Mobile Security
   6.5. Password Protection
   6.6. Phishing
   6.7. Physical Security
   6.8. Safe Web Browsing
   6.9. Security Beyond the Office
   6.10. Security Essentials
   6.11. Social Engineering
7. The solutions provider must provide phishing simulation tool which allows custom templates to include company images including logos and informative content to the training campaign notification email.

B. SOLUTIONS PLATFORM REQUIREMENT

Summary List of Required Licenses, Equipment and Services:	
Solutions	Technical Specifications
Endpoint Protection (Workstations)	4750 endpoints



Managed Detection and Response plus Remediation

Terms of Reference

Endpoint Detection and Response	5500 sensors
Server Protection	750 servers
Network Detection and Response *	2 units with 1Gbps each of traffic inspection
Network Threat Prevention/IPS (Intrusion Prevention System) *	1 unit – 10Gb inspection throughput; 2 segment 100GbE with bypass option
Cloud Email Security	5000 mailbox
Security Awareness (Phishing Simulation)	500 users
CSOC Layout	1 Lot

* All facility/solution components (servers/nodes) must be equipped with dual power supplies. This ensures power redundancy and enhances system availability in the event of a power source failure.

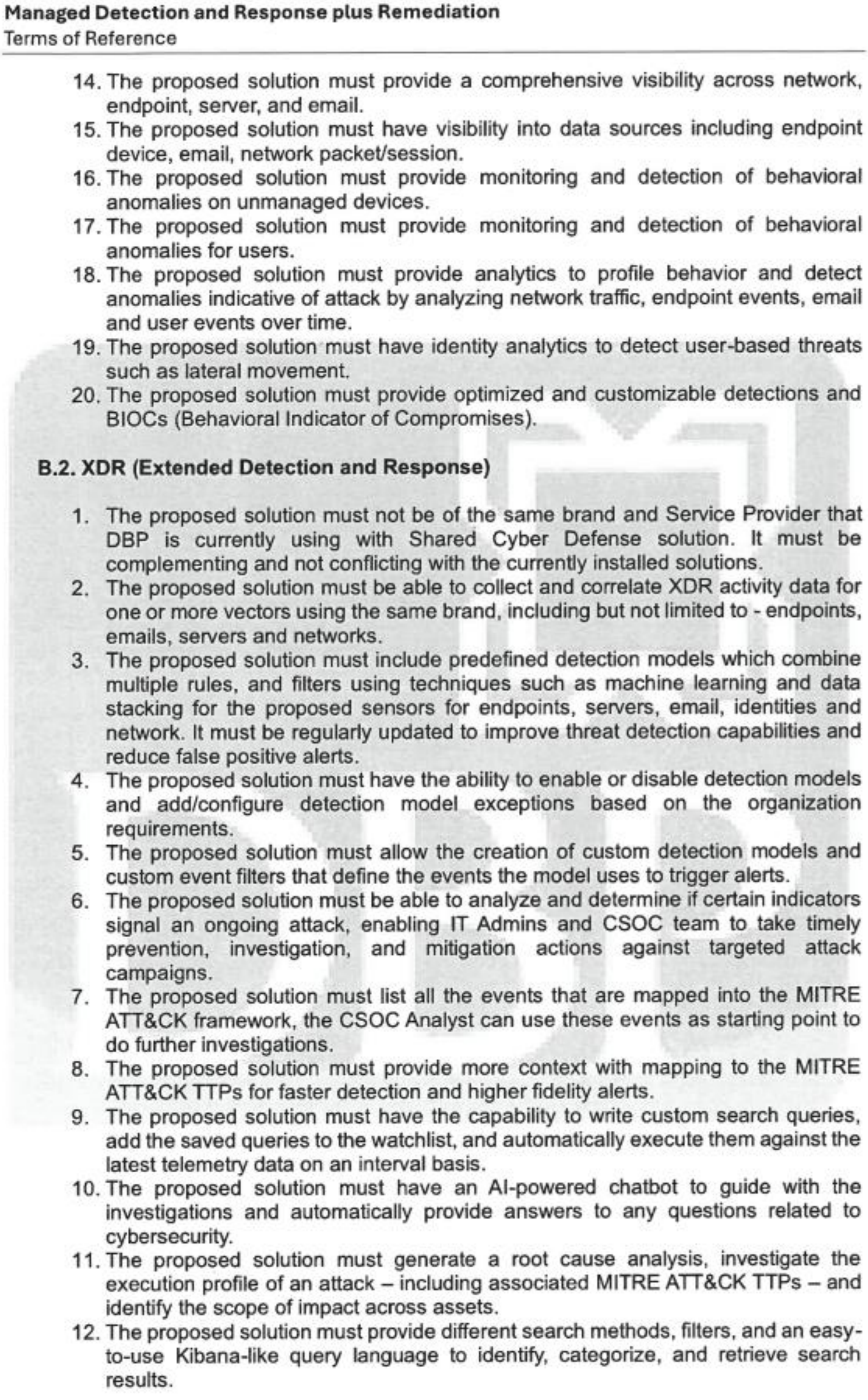
* Any facility/solution components (servers/nodes) that requires a direct connection to the core switch—based on its designated function or operation demands—must be equipped with a network interface supporting a minimum throughput of 10Gbps. This ensures compatibility with existing network infrastructure.

B.1. Threat Detection and Continuous Monitoring

1. Threat Hunting and Threat Intelligence

2. The proposed solution must be able to monitor for advanced threat protection security alerts, breaches, anomalies and advanced persistent threats within the scope of licenses installed under this project.
3. The proposed solution must have defined hunting techniques that are implemented using the capabilities from existing Bank's Anti-APT (Advanced Persistent Threats) technologies, proposed EDR (Endpoint Detection and Response), Email Sensor and Network Forensic device.
4. The proposed solution must provide a 24x7x365 Managed Threat Hunting Service.
5. The proposed solution must conduct continuous Vulnerability Management, Phishing Simulation Exercises and (IR) Incident Response as needed.
6. The proposed solution must have proven and established protocols for threat hunting, defined threat hunting process and triggers for threat hunts and hunt success measurement.
7. The proposed solution must conduct threat hunting based on analysis of suspicious signals, custom detection rules, and internal threat intelligence research.
8. The proposed solution must contain active threats detected, by isolating endpoints and removing malicious files or processes.
9. The proposed solution must provide integration with threat intelligence feeds for the identification of IoC (Indicators of Compromise).
10. The proposed solution must have defined indicators that will trigger a proactive threat hunt.
11. The proposed solution must support sharing of IoCs across multivendor security stack.
12. The proposed solution must provide proactive threat reports for verified threats and/or provide emerging threat reports on emerging threats affecting multiple organizations, designed to help the organization stay ahead of high-profile cyber-attacks.

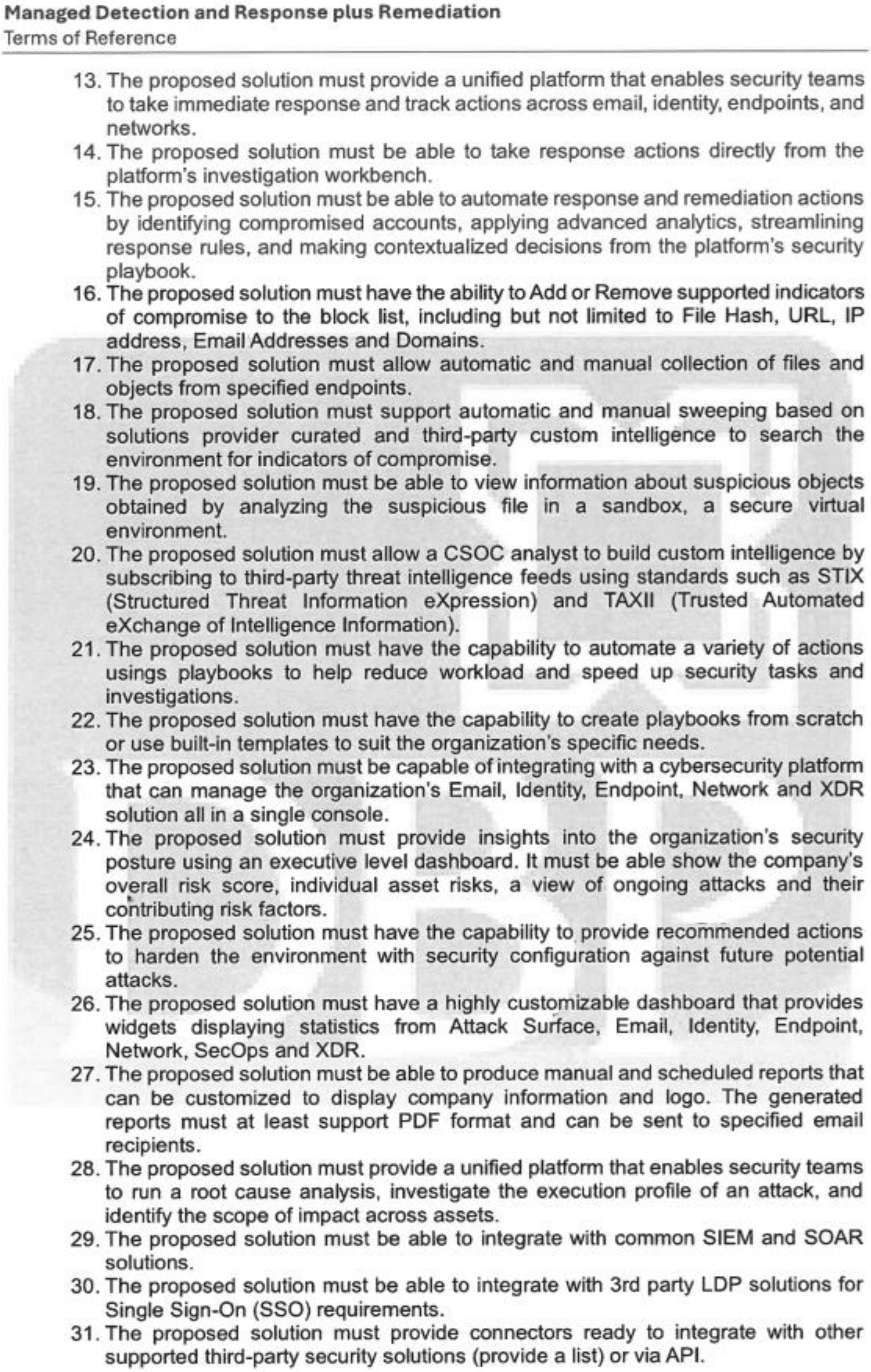
13. Visibility and Detection



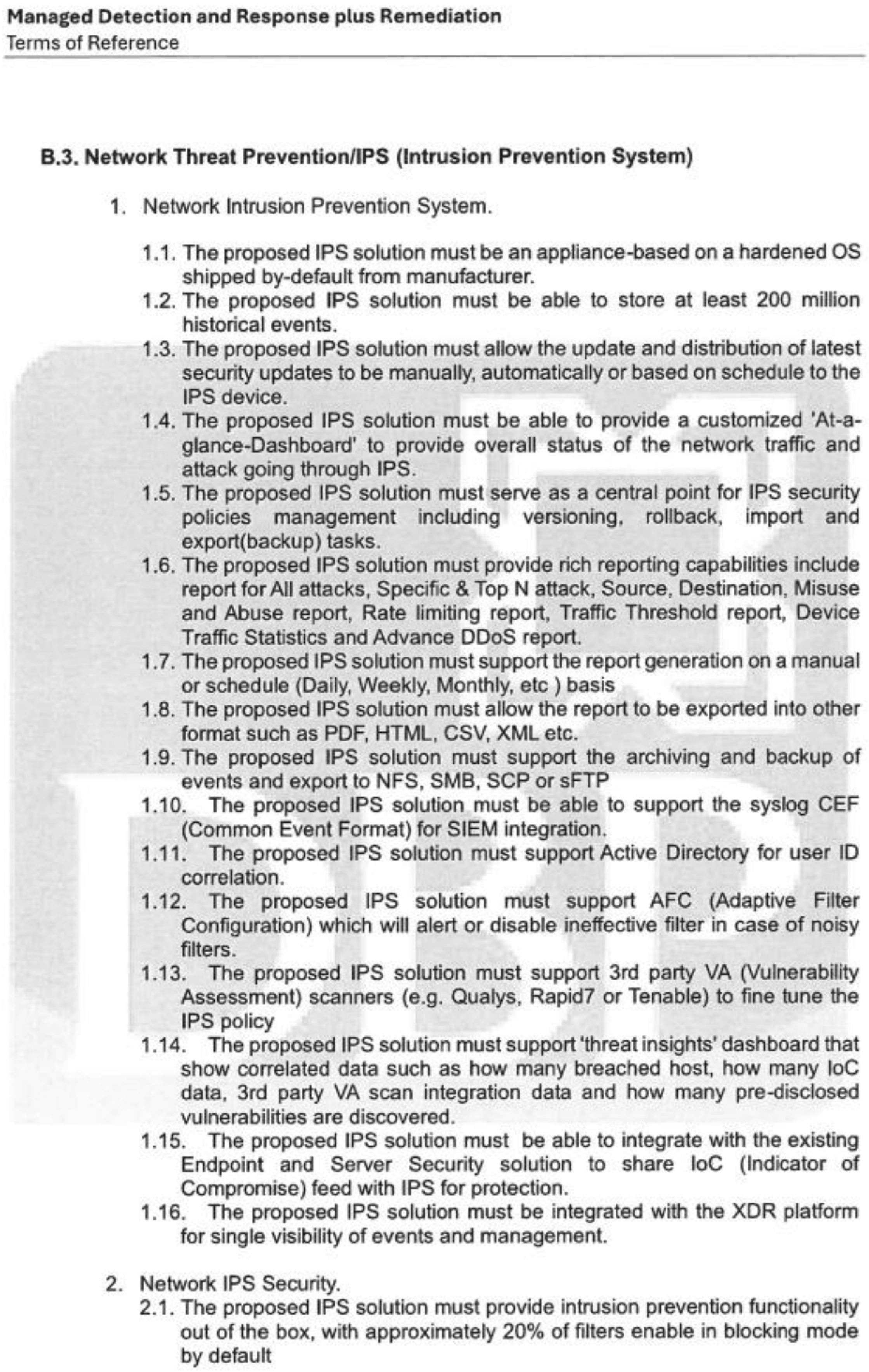
14. The proposed solution must provide a comprehensive visibility across network, endpoint, server, and email.
15. The proposed solution must have visibility into data sources including endpoint device, email, network packet/session.
16. The proposed solution must provide monitoring and detection of behavioral anomalies on unmanaged devices.
17. The proposed solution must provide monitoring and detection of behavioral anomalies for users.
18. The proposed solution must provide analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, email and user events over time.
19. The proposed solution must have identity analytics to detect user-based threats such as lateral movement.
20. The proposed solution must provide optimized and customizable detections and BIOCs (Behavioral Indicator of Compromises).

B.2. XDR (Extended Detection and Response)

1. The proposed solution must not be of the same brand and Service Provider that DBP is currently using with Shared Cyber Defense solution. It must be complementing and not conflicting with the currently installed solutions.
2. The proposed solution must be able to collect and correlate XDR activity data for one or more vectors using the same brand, including but not limited to - endpoints, emails, servers and networks.
3. The proposed solution must include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking for the proposed sensors for endpoints, servers, email, identities and network. It must be regularly updated to improve threat detection capabilities and reduce false positive alerts.
4. The proposed solution must have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements.
5. The proposed solution must allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.
6. The proposed solution must be able to analyze and determine if certain indicators signal an ongoing attack, enabling IT Admins and CSOC team to take timely prevention, investigation, and mitigation actions against targeted attack campaigns.
7. The proposed solution must list all the events that are mapped into the MITRE ATT&CK framework, the CSOC Analyst can use these events as starting point to do further investigations.
8. The proposed solution must provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.
9. The proposed solution must have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.
10. The proposed solution must have an AI-powered chatbot to guide with the investigations and automatically provide answers to any questions related to cybersecurity.
11. The proposed solution must generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.
12. The proposed solution must provide different search methods, filters, and an easy-to-use Kibana-like query language to identify, categorize, and retrieve search results.



13. The proposed solution must provide a unified platform that enables security teams to take immediate response and track actions across email, identity, endpoints, and networks.
14. The proposed solution must be able to take response actions directly from the platform's investigation workbench.
15. The proposed solution must be able to automate response and remediation actions by identifying compromised accounts, applying advanced analytics, streamlining response rules, and making contextualized decisions from the platform's security playbook.
16. The proposed solution must have the ability to Add or Remove supported indicators of compromise to the block list, including but not limited to File Hash, URL, IP address, Email Addresses and Domains.
17. The proposed solution must allow automatic and manual collection of files and objects from specified endpoints.
18. The proposed solution must support automatic and manual sweeping based on solutions provider curated and third-party custom intelligence to search the environment for indicators of compromise.
19. The proposed solution must be able to view information about suspicious objects obtained by analyzing the suspicious file in a sandbox, a secure virtual environment.
20. The proposed solution must allow a CSOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Intelligence Information).
21. The proposed solution must have the capability to automate a variety of actions usings playbooks to help reduce workload and speed up security tasks and investigations.
22. The proposed solution must have the capability to create playbooks from scratch or use built-in templates to suit the organization's specific needs.
23. The proposed solution must be capable of integrating with a cybersecurity platform that can manage the organization's Email, Identity, Endpoint, Network and XDR solution all in a single console.
24. The proposed solution must provide insights into the organization's security posture using an executive level dashboard. It must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors.
25. The proposed solution must have the capability to provide recommended actions to harden the environment with security configuration against future potential attacks.
26. The proposed solution must have a highly customizable dashboard that provides widgets displaying statistics from Attack Surface, Email, Identity, Endpoint, Network, SecOps and XDR.
27. The proposed solution must be able to produce manual and scheduled reports that can be customized to display company information and logo. The generated reports must at least support PDF format and can be sent to specified email recipients.
28. The proposed solution must provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.
29. The proposed solution must be able to integrate with common SIEM and SOAR solutions.
30. The proposed solution must be able to integrate with 3rd party LDP solutions for Single Sign-On (SSO) requirements.
31. The proposed solution must provide connectors ready to integrate with other supported third-party security solutions (provide a list) or via API.



B.3. Network Threat Prevention/IPS (Intrusion Prevention System)

1. Network Intrusion Prevention System.

1.1. The proposed IPS solution must be an appliance-based on a hardened OS shipped by-default from manufacturer.

1.2. The proposed IPS solution must be able to store at least 200 million historical events.

1.3. The proposed IPS solution must allow the update and distribution of latest security updates to be manually, automatically or based on schedule to the IPS device.

1.4. The proposed IPS solution must be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through IPS.

1.5. The proposed IPS solution must serve as a central point for IPS security policies management including versioning, rollback, import and export(backup) tasks.

1.6. The proposed IPS solution must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report.

1.7. The proposed IPS solution must support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis

1.8. The proposed IPS solution must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.

1.9. The proposed IPS solution must support the archiving and backup of events and export to NFS, SMB, SCP or sFTP

1.10. The proposed IPS solution must be able to support the syslog CEF (Common Event Format) for SIEM integration.

1.11. The proposed IPS solution must support Active Directory for user ID correlation.

1.12. The proposed IPS solution must support AFC (Adaptive Filter Configuration) which will alert or disable ineffective filter in case of noisy filters.

1.13. The proposed IPS solution must support 3rd party VA (Vulnerability Assessment) scanners (e.g. Qualys, Rapid7 or Tenable) to fine tune the IPS policy

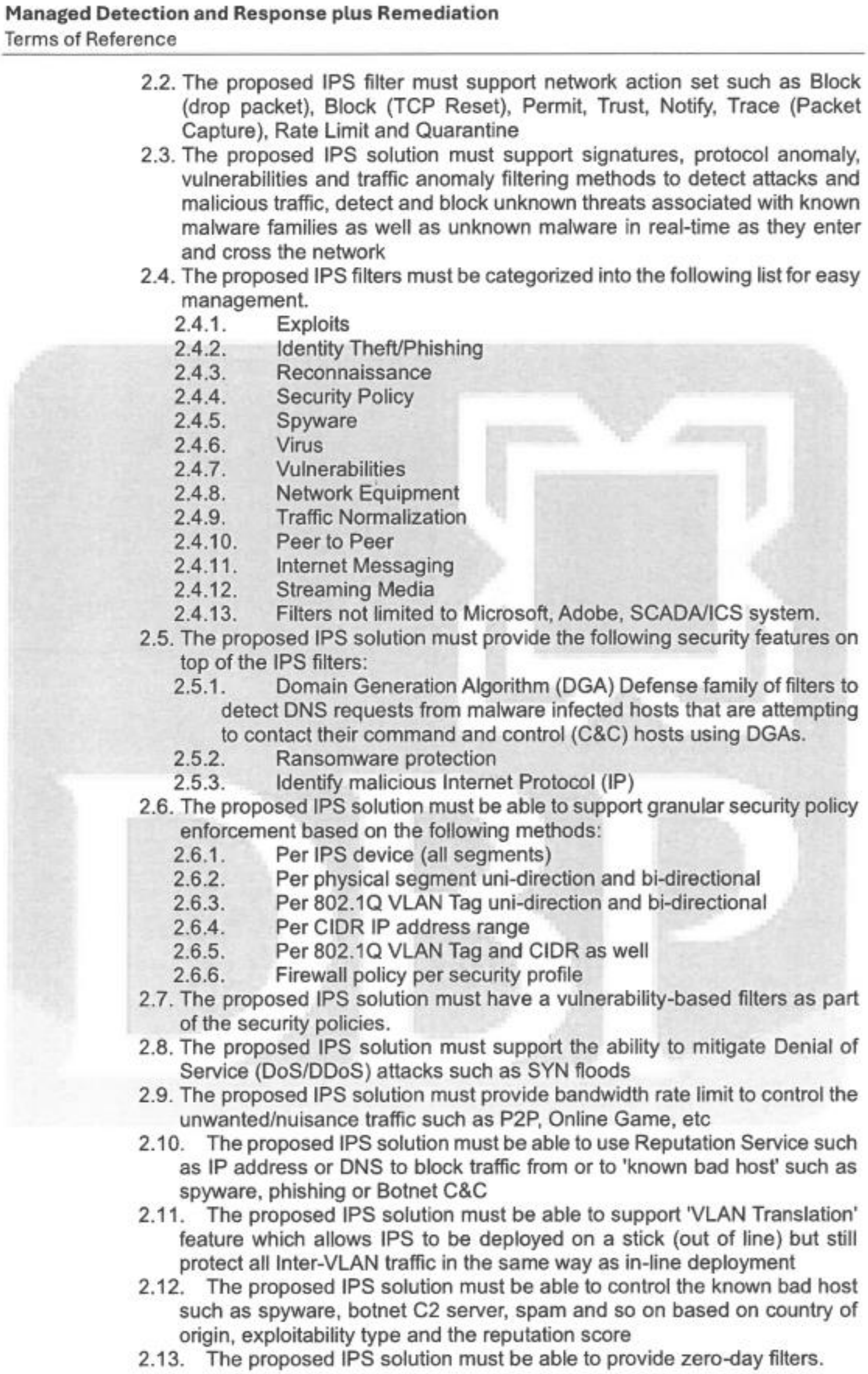
1.14. The proposed IPS solution must support 'threat insights' dashboard that show correlated data such as how many breached host, how many IoC data, 3rd party VA scan integration data and how many pre-disclosed vulnerabilities are discovered.

1.15. The proposed IPS solution must be able to integrate with the existing Endpoint and Server Security solution to share IoC (Indicator of Compromise) feed with IPS for protection.

1.16. The proposed IPS solution must be integrated with the XDR platform for single visibility of events and management.

2. Network IPS Security.

2.1. The proposed IPS solution must provide intrusion prevention functionality out of the box, with approximately 20% of filters enable in blocking mode by default



2.2. The proposed IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine

2.3. The proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic, detect and block unknown threats associated with known malware families as well as unknown malware in real-time as they enter and cross the network

2.4. The proposed IPS filters must be categorized into the following list for easy management.

2.4.1. Exploits
2.4.2. Identity Theft/Phishing
2.4.3. Reconnaissance
2.4.4. Security Policy
2.4.5. Spyware
2.4.6. Virus
2.4.7. Vulnerabilities
2.4.8. Network Equipment
2.4.9. Traffic Normalization
2.4.10. Peer to Peer
2.4.11. Internet Messaging
2.4.12. Streaming Media
2.4.13. Filters not limited to Microsoft, Adobe, SCADA/ICS system.

2.5. The proposed IPS solution must provide the following security features on top of the IPS filters:

2.5.1. Domain Generation Algorithm (DGA) Defense family of filters to detect DNS requests from malware infected hosts that are attempting to contact their command and control (C&C) hosts using DGAs.
2.5.2. Ransomware protection
2.5.3. Identify malicious Internet Protocol (IP)

2.6. The proposed IPS solution must be able to support granular security policy enforcement based on the following methods:

2.6.1. Per IPS device (all segments)
2.6.2. Per physical segment uni-direction and bi-directional
2.6.3. Per 802.1Q VLAN Tag uni-direction and bi-directional
2.6.4. Per CIDR IP address range
2.6.5. Per 802.1Q VLAN Tag and CIDR as well
2.6.6. Firewall policy per security profile

2.7. The proposed IPS solution must have a vulnerability-based filters as part of the security policies.

2.8. The proposed IPS solution must support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods

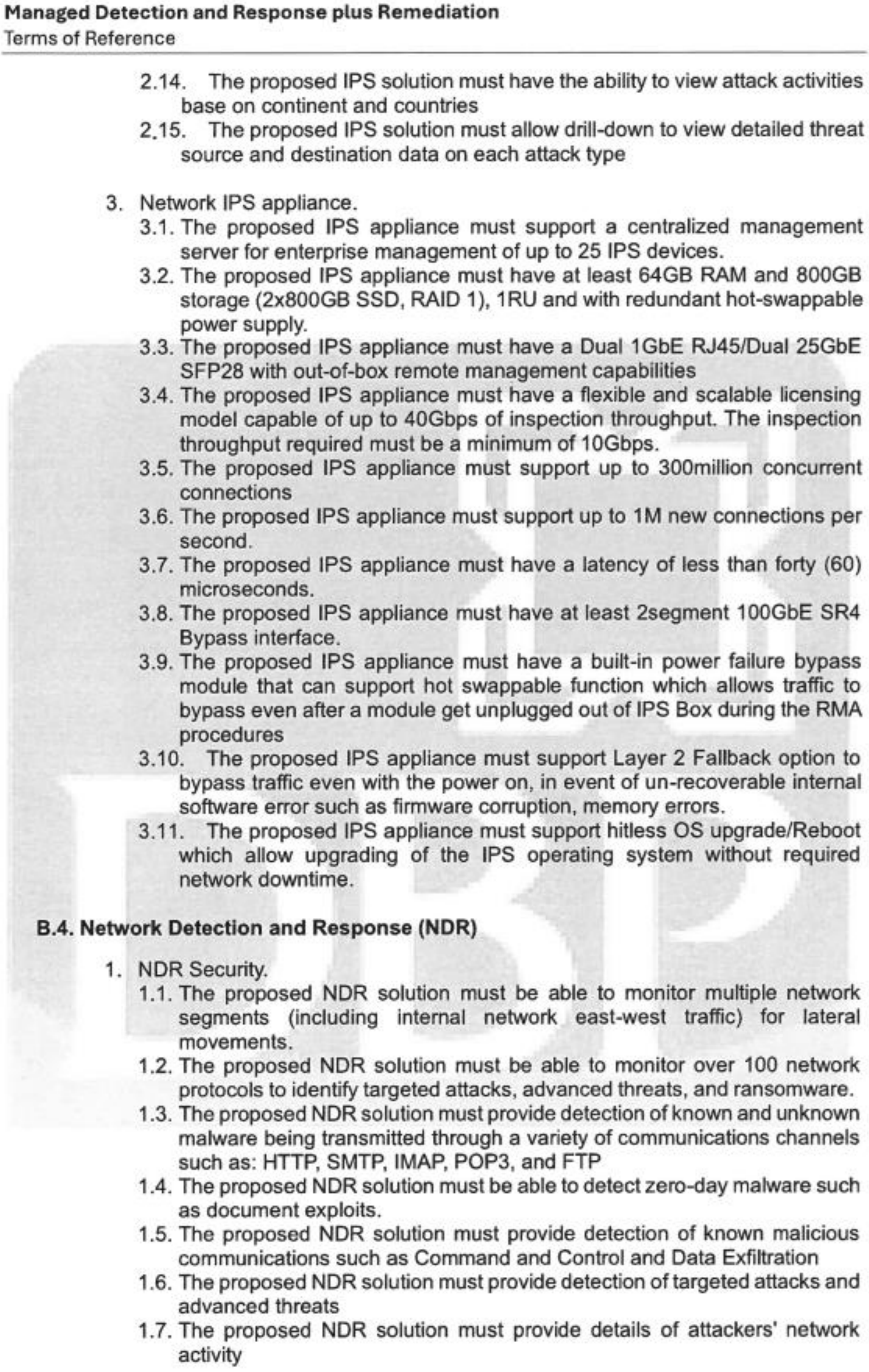
2.9. The proposed IPS solution must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc

2.10. The proposed IPS solution must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C

2.11. The proposed IPS solution must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment

2.12. The proposed IPS solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploitability type and the reputation score

2.13. The proposed IPS solution must be able to provide zero-day filters.



2.14. The proposed IPS solution must have the ability to view attack activities base on continent and countries

2.15. The proposed IPS solution must allow drill-down to view detailed threat source and destination data on each attack type

3. Network IPS appliance.

3.1. The proposed IPS appliance must support a centralized management server for enterprise management of up to 25 IPS devices.

3.2. The proposed IPS appliance must have at least 64GB RAM and 800GB storage (2x800GB SSD, RAID 1), 1RU and with redundant hot-swappable power supply.

3.3. The proposed IPS appliance must have a Dual 1GbE RJ45/Dual 25GbE SFP28 with out-of-box remote management capabilities

3.4. The proposed IPS appliance must have a flexible and scalable licensing model capable of up to 40Gbps of inspection throughput. The inspection throughput required must be a minimum of 10Gbps.

3.5. The proposed IPS appliance must support up to 300million concurrent connections

3.6. The proposed IPS appliance must support up to 1M new connections per second.

3.7. The proposed IPS appliance must have a latency of less than forty (60) microseconds.

3.8. The proposed IPS appliance must have at least 2segment 100GbE SR4 Bypass interface.

3.9. The proposed IPS appliance must have a built-in power failure bypass module that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedures

3.10. The proposed IPS appliance must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors.

3.11. The proposed IPS appliance must support hitless OS upgrade/Reboot which allow upgrading of the IPS operating system without required network downtime.

B.4. Network Detection and Response (NDR)

1. NDR Security.

1.1. The proposed NDR solution must be able to monitor multiple network segments (including internal network east-west traffic) for lateral movements.

1.2. The proposed NDR solution must be able to monitor over 100 network protocols to identify targeted attacks, advanced threats, and ransomware.

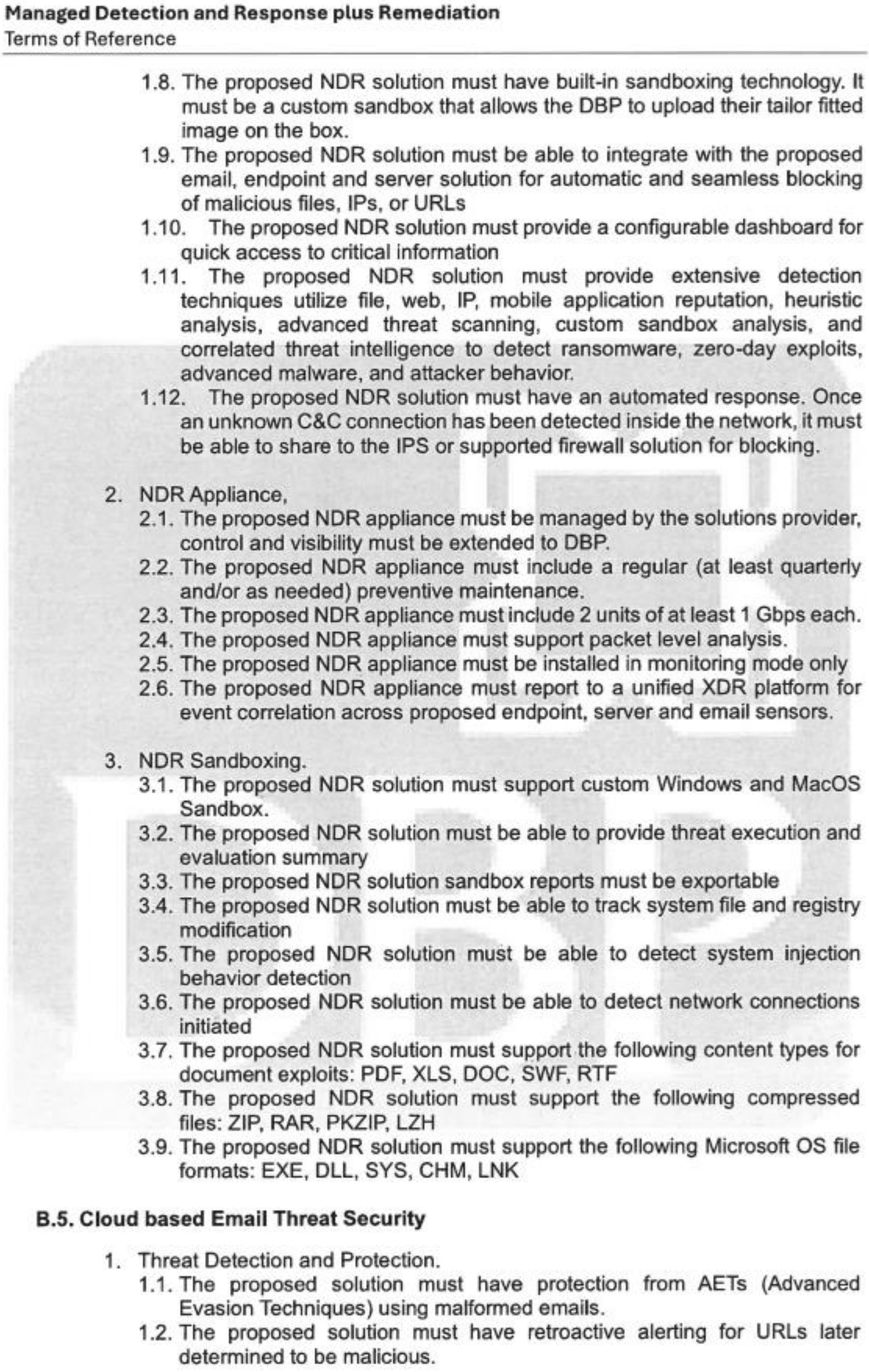
1.3. The proposed NDR solution must provide detection of known and unknown malware being transmitted through a variety of communications channels such as: HTTP, SMTP, IMAP, POP3, and FTP

1.4. The proposed NDR solution must be able to detect zero-day malware such as document exploits.

1.5. The proposed NDR solution must provide detection of known malicious communications such as Command and Control and Data Exfiltration

1.6. The proposed NDR solution must provide detection of targeted attacks and advanced threats

1.7. The proposed NDR solution must provide details of attackers' network activity



1.8. The proposed NDR solution must have built-in sandboxing technology. It must be a custom sandbox that allows the DBP to upload their tailor fitted image on the box.

1.9. The proposed NDR solution must be able to integrate with the proposed email, endpoint and server solution for automatic and seamless blocking of malicious files, IPs, or URLs

1.10. The proposed NDR solution must provide a configurable dashboard for quick access to critical information

1.11. The proposed NDR solution must provide extensive detection techniques utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.

1.12. The proposed NDR solution must have an automated response. Once an unknown C&C connection has been detected inside the network, it must be able to share to the IPS or supported firewall solution for blocking.

2. NDR Appliance,

2.1. The proposed NDR appliance must be managed by the solutions provider, control and visibility must be extended to DBP.

2.2. The proposed NDR appliance must include a regular (at least quarterly and/or as needed) preventive maintenance.

2.3. The proposed NDR appliance must include 2 units of at least 1 Gbps each.

2.4. The proposed NDR appliance must support packet level analysis.

2.5. The proposed NDR appliance must be installed in monitoring mode only

2.6. The proposed NDR appliance must report to a unified XDR platform for event correlation across proposed endpoint, server and email sensors.

3. NDR Sandboxing.

3.1. The proposed NDR solution must support custom Windows and MacOS Sandbox.

3.2. The proposed NDR solution must be able to provide threat execution and evaluation summary

3.3. The proposed NDR solution sandbox reports must be exportable

3.4. The proposed NDR solution must be able to track system file and registry modification

3.5. The proposed NDR solution must be able to detect system injection behavior detection

3.6. The proposed NDR solution must be able to detect network connections initiated

3.7. The proposed NDR solution must support the following content types for document exploits: PDF, XLS, DOC, SWF, RTF

3.8. The proposed NDR solution must support the following compressed files: ZIP, RAR, PKZIP, LZH

3.9. The proposed NDR solution must support the following Microsoft OS file formats: EXE, DLL, SYS, CHM, LNK

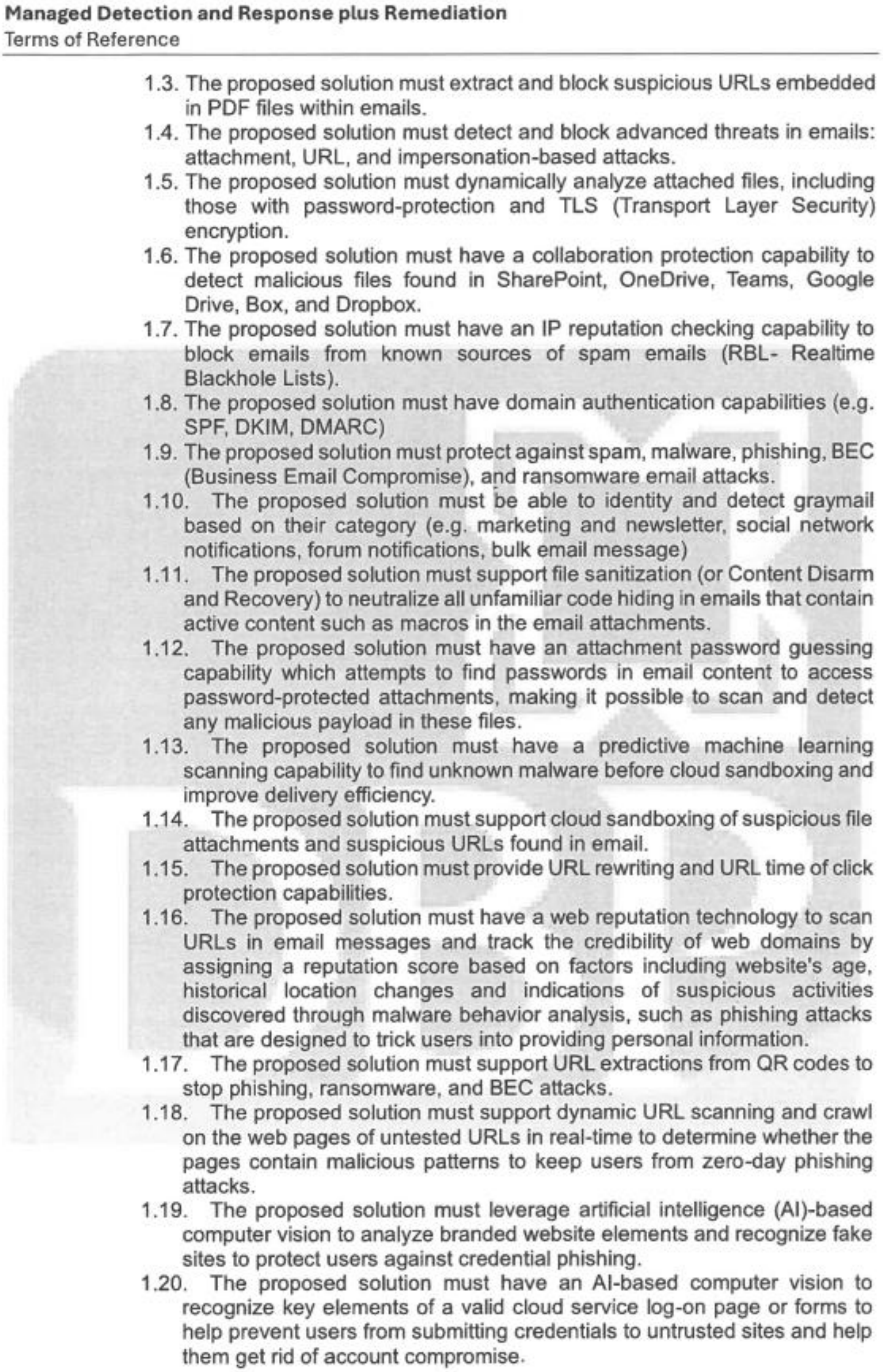
B.5. Cloud based Email Threat Security

1. Threat Detection and Protection.

1.1. The proposed solution must have protection from AETs (Advanced Evasion Techniques) using malformed emails.

1.2. The proposed solution must have retroactive alerting for URLs later determined to be malicious.

FORM 9-A (page 11 of 29)



1.3. The proposed solution must extract and block suspicious URLs embedded in PDF files within emails.

1.4. The proposed solution must detect and block advanced threats in emails: attachment, URL, and impersonation-based attacks.

1.5. The proposed solution must dynamically analyze attached files, including those with password-protection and TLS (Transport Layer Security) encryption.

1.6. The proposed solution must have a collaboration protection capability to detect malicious files found in SharePoint, OneDrive, Teams, Google Drive, Box, and Dropbox.

1.7. The proposed solution must have an IP reputation checking capability to block emails from known sources of spam emails (RBL- Realtime Blackhole Lists).

1.8. The proposed solution must have domain authentication capabilities (e.g. SPF, DKIM, DMARC)

1.9. The proposed solution must protect against spam, malware, phishing, BEC (Business Email Compromise), and ransomware email attacks.

1.10. The proposed solution must be able to identity and detect graymail based on their category (e.g. marketing and newsletter, social network notifications, forum notifications, bulk email message)

1.11. The proposed solution must support file sanitization (or Content Disarm and Recovery) to neutralize all unfamiliar code hiding in emails that contain active content such as macros in the email attachments.

1.12. The proposed solution must have an attachment password guessing capability which attempts to find passwords in email content to access password-protected attachments, making it possible to scan and detect any malicious payload in these files.

1.13. The proposed solution must have a predictive machine learning scanning capability to find unknown malware before cloud sandboxing and improve delivery efficiency.

1.14. The proposed solution must support cloud sandboxing of suspicious file attachments and suspicious URLs found in email.

1.15. The proposed solution must provide URL rewriting and URL time of click protection capabilities.

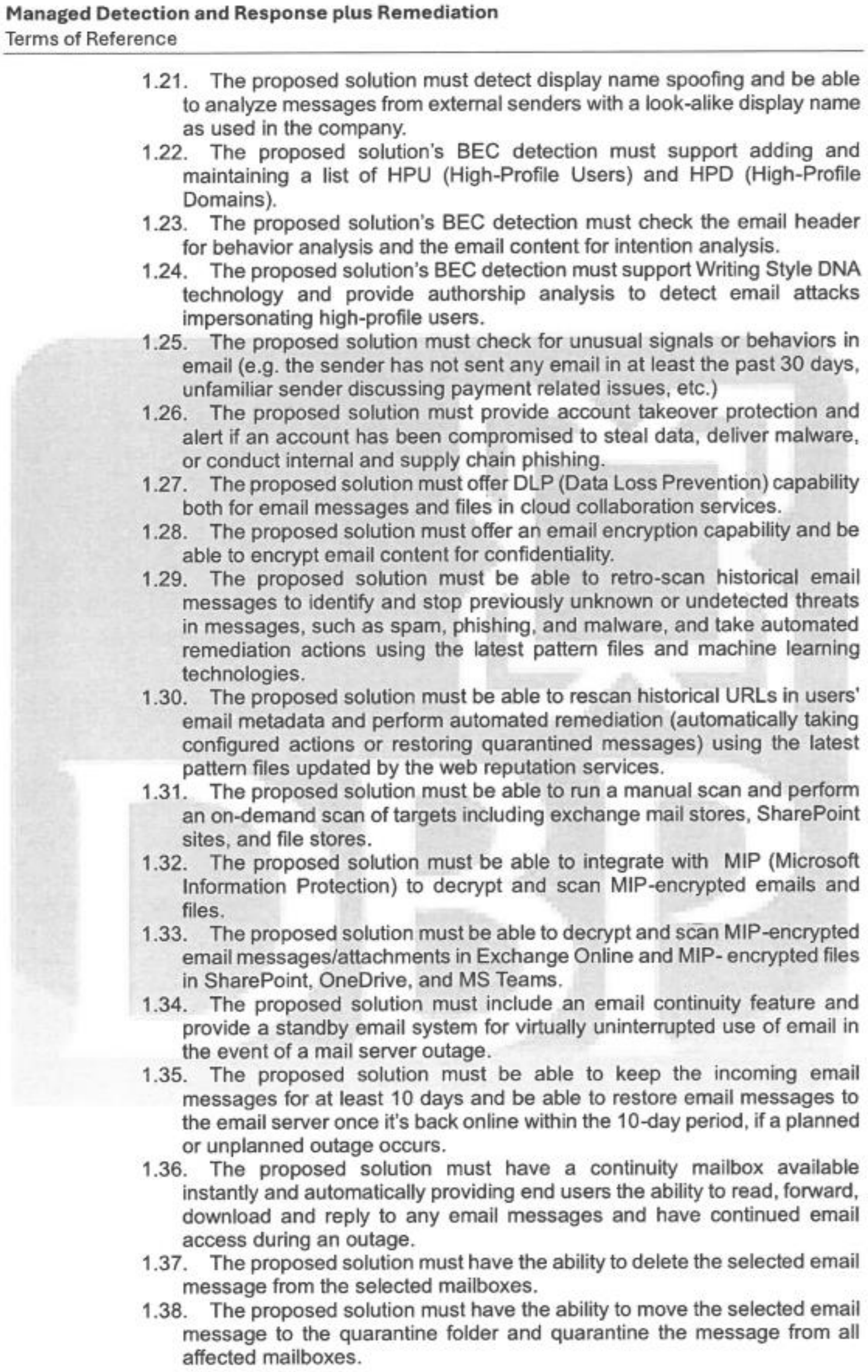
1.16. The proposed solution must have a web reputation technology to scan URLs in email messages and track the credibility of web domains by assigning a reputation score based on factors including website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing attacks that are designed to trick users into providing personal information.

1.17. The proposed solution must support URL extractions from QR codes to stop phishing, ransomware, and BEC attacks.

1.18. The proposed solution must support dynamic URL scanning and crawl on the web pages of untested URLs in real-time to determine whether the pages contain malicious patterns to keep users from zero-day phishing attacks.

1.19. The proposed solution must leverage artificial intelligence (AI)-based computer vision to analyze branded website elements and recognize fake sites to protect users against credential phishing.

1.20. The proposed solution must have an AI-based computer vision to recognize key elements of a valid cloud service log-on page or forms to help prevent users from submitting credentials to untrusted sites and help them get rid of account compromise.



1.21. The proposed solution must detect display name spoofing and be able to analyze messages from external senders with a look-alike display name as used in the company.

1.22. The proposed solution's BEC detection must support adding and maintaining a list of HPU (High-Profile Users) and HPD (High-Profile Domains).

1.23. The proposed solution's BEC detection must check the email header for behavior analysis and the email content for intention analysis.

1.24. The proposed solution's BEC detection must support Writing Style DNA technology and provide authorship analysis to detect email attacks impersonating high-profile users.

1.25. The proposed solution must check for unusual signals or behaviors in email (e.g. the sender has not sent any email in at least the past 30 days, unfamiliar sender discussing payment related issues, etc.)

1.26. The proposed solution must provide account takeover protection and alert if an account has been compromised to steal data, deliver malware, or conduct internal and supply chain phishing.

1.27. The proposed solution must offer DLP (Data Loss Prevention) capability both for email messages and files in cloud collaboration services.

1.28. The proposed solution must offer an email encryption capability and be able to encrypt email content for confidentiality.

1.29. The proposed solution must be able to retro-scan historical email messages to identify and stop previously unknown or undetected threats in messages, such as spam, phishing, and malware, and take automated remediation actions using the latest pattern files and machine learning technologies.

1.30. The proposed solution must be able to rescan historical URLs in users' email metadata and perform automated remediation (automatically taking configured actions or restoring quarantined messages) using the latest pattern files updated by the web reputation services.

1.31. The proposed solution must be able to run a manual scan and perform an on-demand scan of targets including exchange mail stores, SharePoint sites, and file stores.

1.32. The proposed solution must be able to integrate with MIP (Microsoft Information Protection) to decrypt and scan MIP-encrypted emails and files.

1.33. The proposed solution must be able to decrypt and scan MIP-encrypted email messages/attachments in Exchange Online and MIP- encrypted files in SharePoint, OneDrive, and MS Teams.

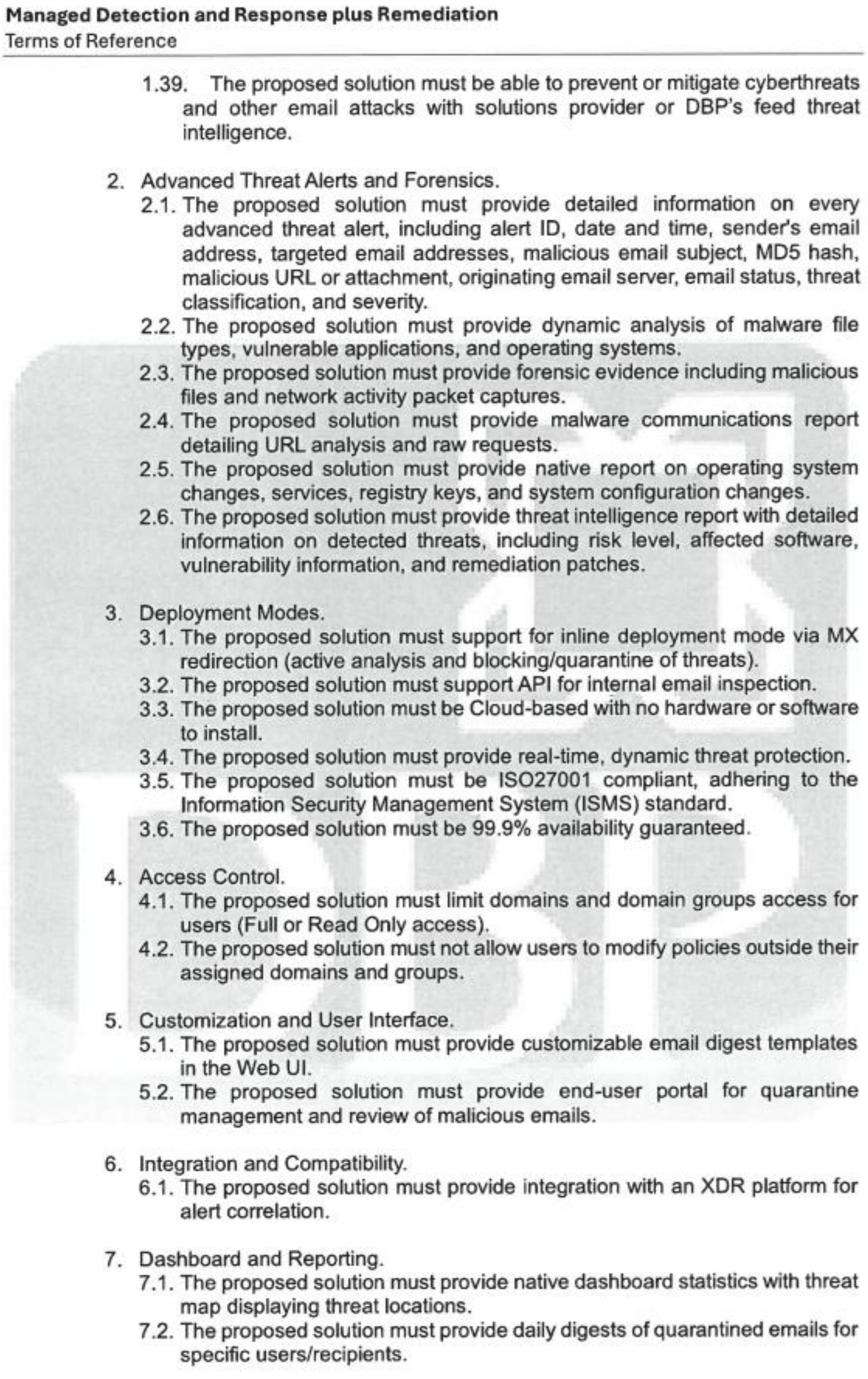
1.34. The proposed solution must include an email continuity feature and provide a standby email system for virtually uninterrupted use of email in the event of a mail server outage.

1.35. The proposed solution must be able to keep the incoming email messages for at least 10 days and be able to restore email messages to the email server once it's back online within the 10-day period, if a planned or unplanned outage occurs.

1.36. The proposed solution must have a continuity mailbox available instantly and automatically providing end users the ability to read, forward, download and reply to any email messages and have continued email access during an outage.

1.37. The proposed solution must have the ability to delete the selected email message from the selected mailboxes.

1.38. The proposed solution must have the ability to move the selected email message to the quarantine folder and quarantine the message from all affected mailboxes.



1.39. The proposed solution must be able to prevent or mitigate cyberthreats and other email attacks with solutions provider or DBP's feed threat intelligence.

2. Advanced Threat Alerts and Forensics.
   - 2.1. The proposed solution must provide detailed information on every advanced threat alert, including alert ID, date and time, sender's email address, targeted email addresses, malicious email subject, MD5 hash, malicious URL or attachment, originating email server, email status, threat classification, and severity.
   - 2.2. The proposed solution must provide dynamic analysis of malware file types, vulnerable applications, and operating systems.
   - 2.3. The proposed solution must provide forensic evidence including malicious files and network activity packet captures.
   - 2.4. The proposed solution must provide malware communications report detailing URL analysis and raw requests.
   - 2.5. The proposed solution must provide native report on operating system changes, services, registry keys, and system configuration changes.
   - 2.6. The proposed solution must provide threat intelligence report with detailed information on detected threats, including risk level, affected software, vulnerability information, and remediation patches.

3. Deployment Modes.
   - 3.1. The proposed solution must support for inline deployment mode via MX redirection (active analysis and blocking/quarantine of threats).
   - 3.2. The proposed solution must support API for internal email inspection.
   - 3.3. The proposed solution must be Cloud-based with no hardware or software to install.
   - 3.4. The proposed solution must provide real-time, dynamic threat protection.
   - 3.5. The proposed solution must be ISO27001 compliant, adhering to the Information Security Management System (ISMS) standard.
   - 3.6. The proposed solution must be 99.9% availability guaranteed.

4. Access Control.
   - 4.1. The proposed solution must limit domains and domain groups access for users (Full or Read Only access).
   - 4.2. The proposed solution must not allow users to modify policies outside their assigned domains and groups.

5. Customization and User Interface.
   - 5.1. The proposed solution must provide customizable email digest templates in the Web UI.
   - 5.2. The proposed solution must provide end-user portal for quarantine management and review of malicious emails.

6. Integration and Compatibility.
   - 6.1. The proposed solution must provide integration with an XDR platform for alert correlation.

7. Dashboard and Reporting.
   - 7.1. The proposed solution must provide native dashboard statistics with threat map displaying threat locations.
   - 7.2. The proposed solution must provide daily digests of quarantined emails for specific users/recipients.

7.3. The proposed solution must provide executive summary report of email traffic, content analysis, and threat categories.

8. Email Handling Rules.

8.1. The proposed solution must provide creation of allow and deny rules based on criteria such as reverse DNS validation, sender country internet domain suffix, recipient email address, sender IP address, sender email address, and sender email domain.

8.2. The proposed solution must have the ability to drop, quarantine, deliver, route, BCC (Blind Carbon Copy), insert custom headers, and modify the subject of emails based on specific criteria.

8.3. The proposed solution must have the ability to bypass antivirus and antispam scanning based on specific criteria.

9. File Type Analysis.

9.1. The proposed solution must provide dynamic analysis of attached file types and/or extensions such as EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives.

B.6. Server Security and Protection.

1. General Server Security.

1.1. The proposed solution must have an option for on-premise management for server protection over physical and virtual servers.

1.2. The proposed solution must allow the on-premise management server to connection to a cloud-based unified XDR platform.

1.3. The proposed solution must provide layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.

1.4. The proposed solution must protect a wide range of platforms including but not limited to: AIX, AlmaLinux, Amazon Linux, CentOS, CloudLinux, Debian, Oracle Linux, RHEL, Micracle Linux, Red Hat OpenShift, Rocky Linux, Solaris, SUSE Linux, Ubuntu Linux and Windows including legacy OS.

1.5. The proposed solution must have multiple security modules listed below, providing a line of defense at the server in a single agent:

1.5.1. Anti-Malware

1.5.1.1. The proposed anti-malware solution must provide agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, trojans, and spyware.

1.5.1.2. The proposed anti-malware solution must allow manual and schedule scans to be configured.

1.5.1.3. The proposed anti-malware solution must be able to provide Web Reputation filtering to protect against malicious web sites

1.5.1.4. The proposed anti-malware solution must have an option to configure its detection and prevention level from cautious, moderate to aggressive and extra aggressive for its protection capabilities.

1.5.1.5. The proposed anti-malware solution must have Predictive Machine Learning to protect against unknown malware.

1.5.1.6. The proposed anti-malware solution must have behavioral monitoring to protect against suspicious activity and unauthorized changes including ransomware.

1.5.1.7. The proposed anti-malware solution must provide ransomware protection, that can backup & restore encrypted documents.

1.5.1.8. The proposed anti-malware solution must scan process memory for malware.

1.5.2. Device Control

1.5.2.1. The proposed device control solution must support USB mass storage, autorun function and mobile – MTP (Media Transfer Protocol) /PTP (Picture Transfer Protocol).

1.5.2.2. The proposed device control solution must have option to choose from full access, read only and block.

1.5.3. Intrusion Detection and Prevention System

1.5.3.1. The proposed solution must be able to provide HIPS (Host Intrusion Prevention System) /HIDS (Host-Based Intrusion Detection System) features.

1.5.3.2. The proposed solution must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.

1.5.3.3. The proposed solution must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.

1.5.3.4. The proposed solution must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.

1.5.3.5. The proposed solution must be able to provide protection against known and zero-day attacks

1.5.3.6. The proposed solution must provide protection that can be pushed out to thousands of servers in minutes without a system reboot.

1.5.3.7. The proposed solution must include out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services.

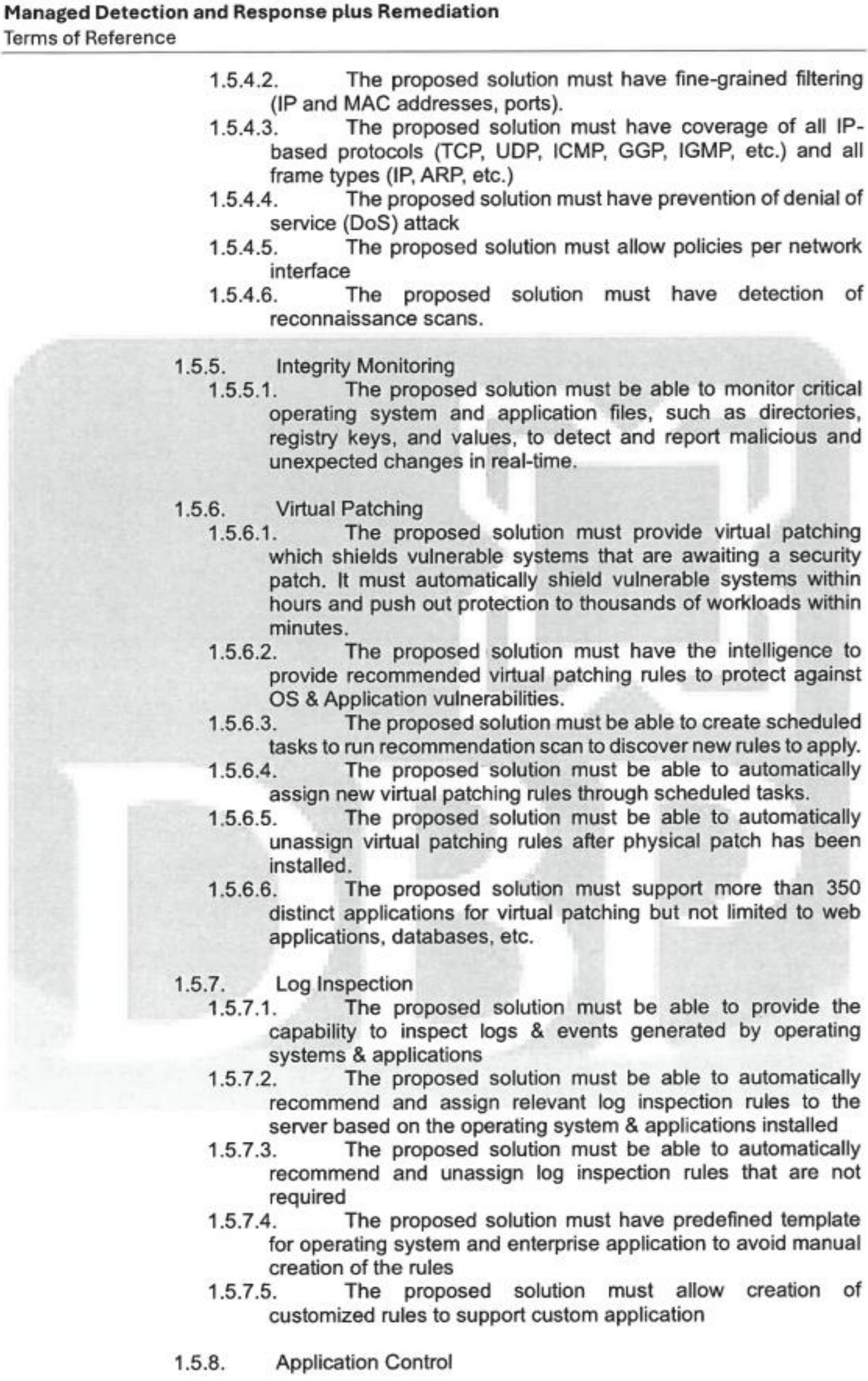
1.5.3.8. The proposed solution must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code

1.5.3.9. The proposed solution must include exploit rules to stop known attacks and malwares.

1.5.3.10. The proposed solution must assist in compliance of PCI DSS (Payment Card Industry Data Security Standard) to protect web applications and the data being process.

1.5.4. Firewall

1.5.4.1. The proposed solution must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.



1.5.4.2. The proposed solution must have fine-grained filtering (IP and MAC addresses, ports).

1.5.4.3. The proposed solution must have coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)

1.5.4.4. The proposed solution must have prevention of denial of service (DoS) attack

1.5.4.5. The proposed solution must allow policies per network interface

1.5.4.6. The proposed solution must have detection of reconnaissance scans.

1.5.5. Integrity Monitoring

1.5.5.1. The proposed solution must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real-time.

1.5.6. Virtual Patching

1.5.6.1. The proposed solution must provide virtual patching which shields vulnerable systems that are awaiting a security patch. It must automatically shield vulnerable systems within hours and push out protection to thousands of workloads within minutes.

1.5.6.2. The proposed solution must have the intelligence to provide recommended virtual patching rules to protect against OS & Application vulnerabilities.

1.5.6.3. The proposed solution must be able to create scheduled tasks to run recommendation scan to discover new rules to apply.

1.5.6.4. The proposed solution must be able to automatically assign new virtual patching rules through scheduled tasks.

1.5.6.5. The proposed solution must be able to automatically unassign virtual patching rules after physical patch has been installed.

1.5.6.6. The proposed solution must support more than 350 distinct applications for virtual patching but not limited to web applications, databases, etc.

1.5.7. Log Inspection

1.5.7.1. The proposed solution must be able to provide the capability to inspect logs & events generated by operating systems & applications

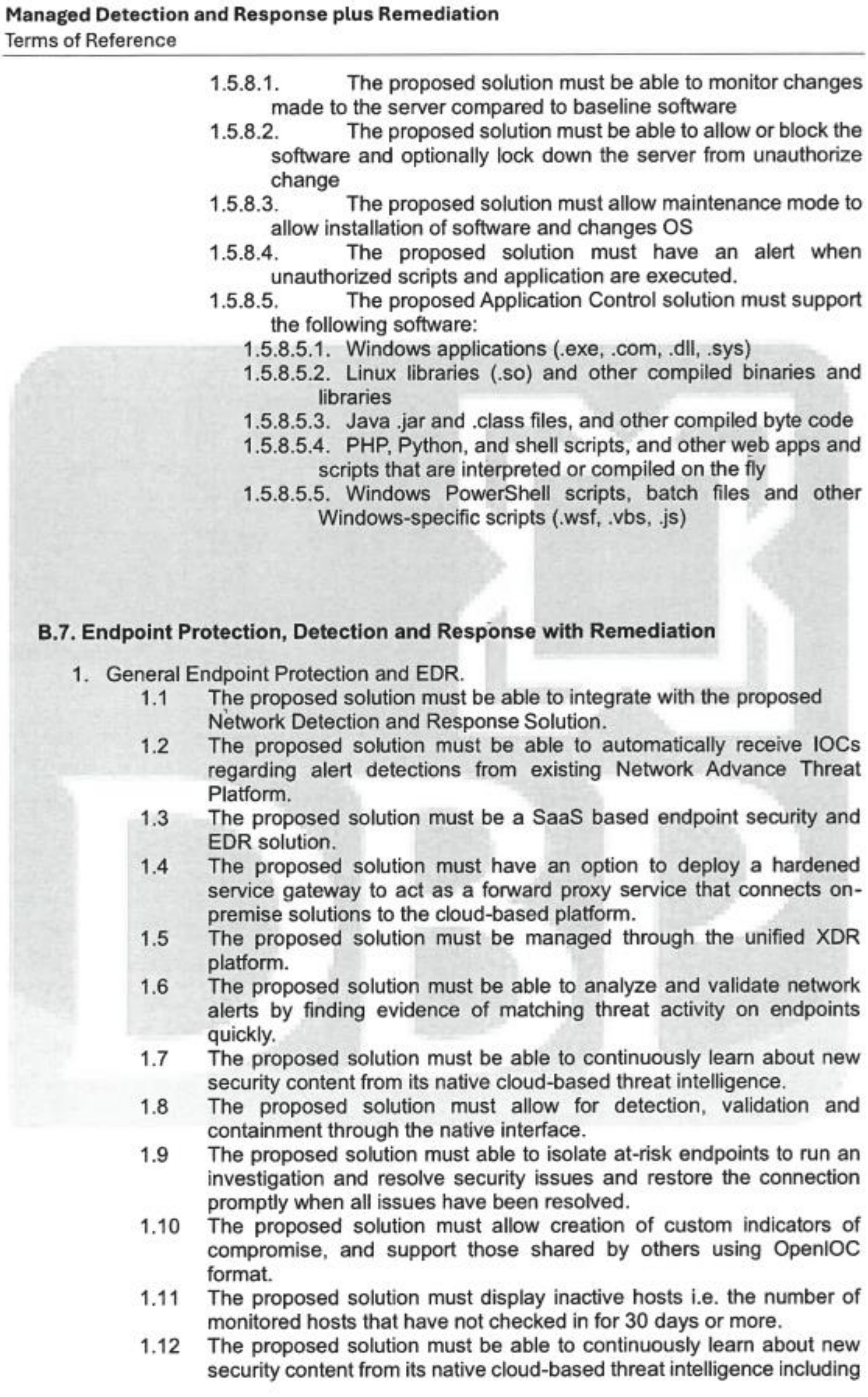
1.5.7.2. The proposed solution must be able to automatically recommend and assign relevant log inspection rules to the server based on the operating system & applications installed

1.5.7.3. The proposed solution must be able to automatically recommend and unassign log inspection rules that are not required

1.5.7.4. The proposed solution must have predefined template for operating system and enterprise application to avoid manual creation of the rules

1.5.7.5. The proposed solution must allow creation of customized rules to support custom application

1.5.8. Application Control



1.5.8.1. The proposed solution must be able to monitor changes made to the server compared to baseline software

1.5.8.2. The proposed solution must be able to allow or block the software and optionally lock down the server from unauthorize change

1.5.8.3. The proposed solution must allow maintenance mode to allow installation of software and changes OS

1.5.8.4. The proposed solution must have an alert when unauthorized scripts and application are executed.

1.5.8.5. The proposed Application Control solution must support the following software:

1.5.8.5.1. Windows applications (.exe, .com, .dll, .sys)

1.5.8.5.2. Linux libraries (.so) and other compiled binaries and libraries

1.5.8.5.3. Java .jar and .class files, and other compiled byte code

1.5.8.5.4. PHP, Python, and shell scripts, and other web apps and scripts that are interpreted or compiled on the fly

1.5.8.5.5. Windows PowerShell scripts, batch files and other Windows-specific scripts (.wsf, .vbs, .js)

B.7. Endpoint Protection, Detection and Response with Remediation

1. General Endpoint Protection and EDR.

1.1 The proposed solution must be able to integrate with the proposed Network Detection and Response Solution.

1.2 The proposed solution must be able to automatically receive IOCs regarding alert detections from existing Network Advance Threat Platform.

1.3 The proposed solution must be a SaaS based endpoint security and EDR solution.

1.4 The proposed solution must have an option to deploy a hardened service gateway to act as a forward proxy service that connects on-premise solutions to the cloud-based platform.

1.5 The proposed solution must be managed through the unified XDR platform.

1.6 The proposed solution must be able to analyze and validate network alerts by finding evidence of matching threat activity on endpoints quickly.

1.7 The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence.

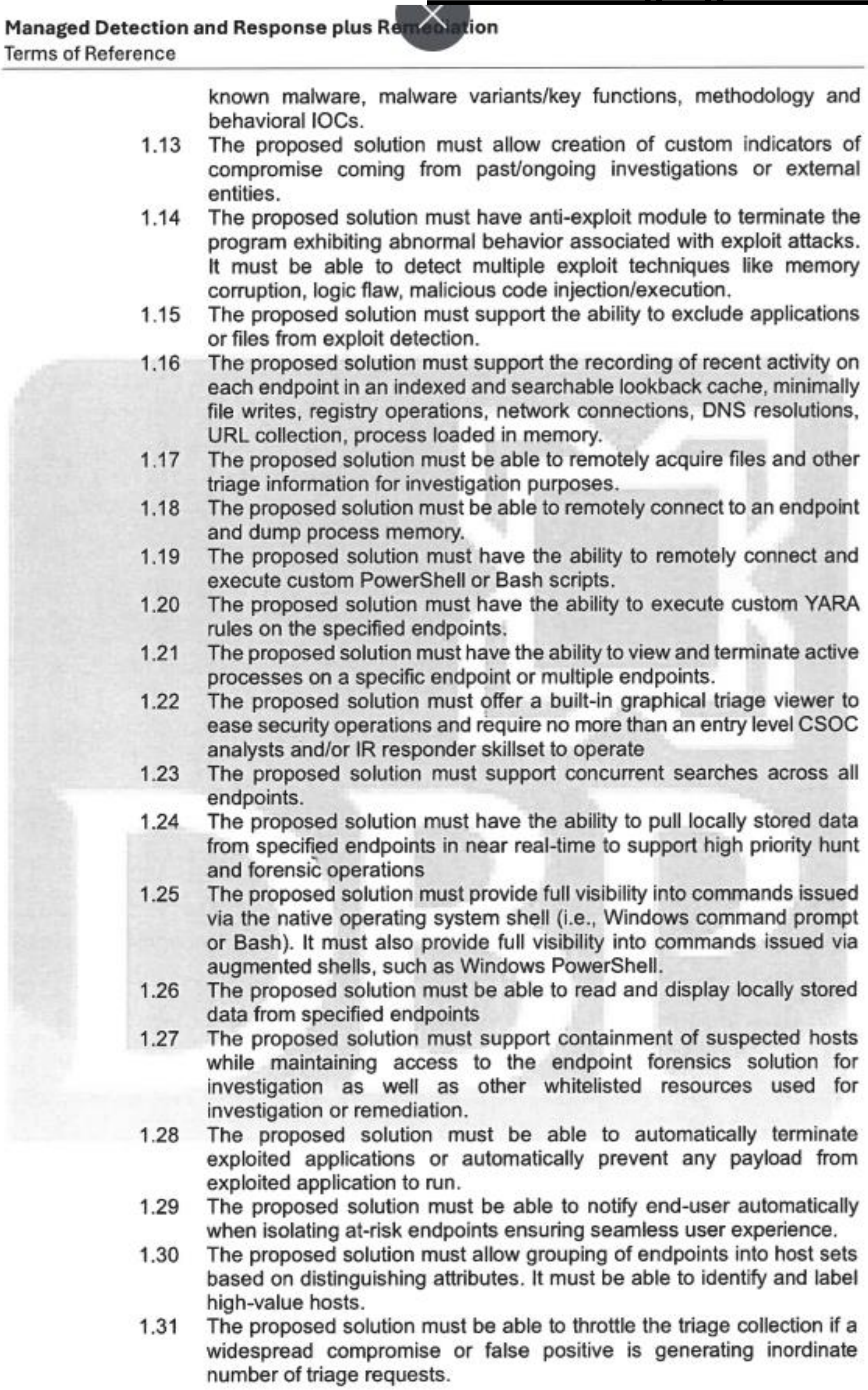
1.8 The proposed solution must allow for detection, validation and containment through the native interface.

1.9 The proposed solution must able to isolate at-risk endpoints to run an investigation and resolve security issues and restore the connection promptly when all issues have been resolved.

1.10 The proposed solution must allow creation of custom indicators of compromise, and support those shared by others using OpenIOC format.

1.11 The proposed solution must display inactive hosts i.e. the number of monitored hosts that have not checked in for 30 days or more.

1.12 The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence including



known malware, malware variants/key functions, methodology and behavioral IOCs.

1.13 The proposed solution must allow creation of custom indicators of compromise coming from past/ongoing investigations or external entities.

1.14 The proposed solution must have anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. It must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.

1.15 The proposed solution must support the ability to exclude applications or files from exploit detection.

1.16 The proposed solution must support the recording of recent activity on each endpoint in an indexed and searchable lookback cache, minimally file writes, registry operations, network connections, DNS resolutions, URL collection, process loaded in memory.

1.17 The proposed solution must be able to remotely acquire files and other triage information for investigation purposes.

1.18 The proposed solution must be able to remotely connect to an endpoint and dump process memory.

1.19 The proposed solution must have the ability to remotely connect and execute custom PowerShell or Bash scripts.

1.20 The proposed solution must have the ability to execute custom YARA rules on the specified endpoints.

1.21 The proposed solution must have the ability to view and terminate active processes on a specific endpoint or multiple endpoints.

1.22 The proposed solution must offer a built-in graphical triage viewer to ease security operations and require no more than an entry level CSOC analysts and/or IR responder skillset to operate

1.23 The proposed solution must support concurrent searches across all endpoints.

1.24 The proposed solution must have the ability to pull locally stored data from specified endpoints in near real-time to support high priority hunt and forensic operations

1.25 The proposed solution must provide full visibility into commands issued via the native operating system shell (i.e., Windows command prompt or Bash). It must also provide full visibility into commands issued via augmented shells, such as Windows PowerShell.

1.26 The proposed solution must be able to read and display locally stored data from specified endpoints

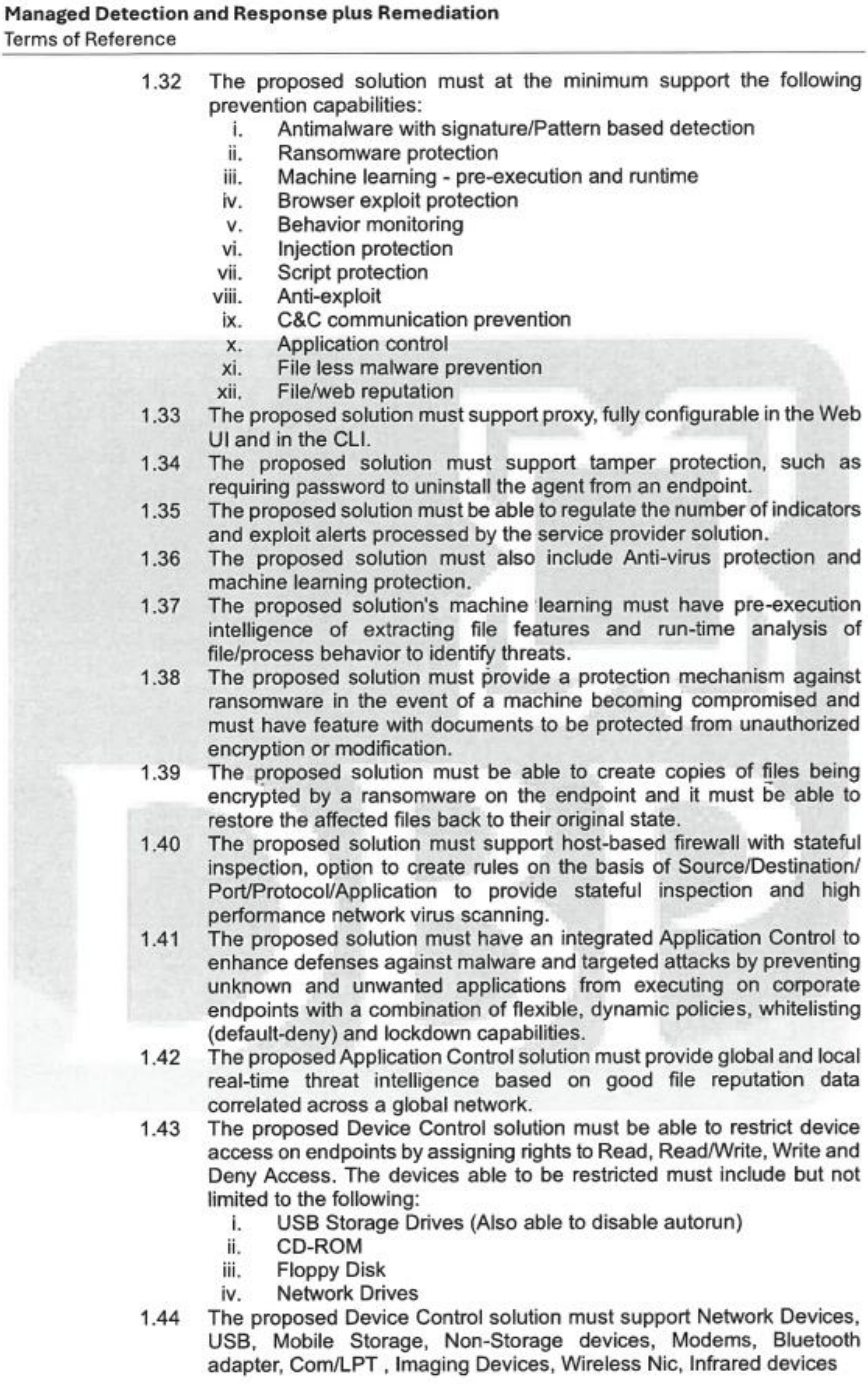
1.27 The proposed solution must support containment of suspected hosts while maintaining access to the endpoint forensics solution for investigation as well as other whitelisted resources used for investigation or remediation.

1.28 The proposed solution must be able to automatically terminate exploited applications or automatically prevent any payload from exploited application to run.

1.29 The proposed solution must be able to notify end-user automatically when isolating at-risk endpoints ensuring seamless user experience.

1.30 The proposed solution must allow grouping of endpoints into host sets based on distinguishing attributes. It must be able to identify and label high-value hosts.

1.31 The proposed solution must be able to throttle the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests.



1.32 The proposed solution must at the minimum support the following prevention capabilities:

i. Antimalware with signature/Pattern based detection
ii. Ransomware protection
iii. Machine learning - pre-execution and runtime
iv. Browser exploit protection
v. Behavior monitoring
vi. Injection protection
vii. Script protection
viii. Anti-exploit
ix. C&C communication prevention
x. Application control
xi. File less malware prevention
xii. File/web reputation

1.33 The proposed solution must support proxy, fully configurable in the Web UI and in the CLI.

1.34 The proposed solution must support tamper protection, such as requiring password to uninstall the agent from an endpoint.

1.35 The proposed solution must be able to regulate the number of indicators and exploit alerts processed by the service provider solution.

1.36 The proposed solution must also include Anti-virus protection and machine learning protection.

1.37 The proposed solution's machine learning must have pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.

1.38 The proposed solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and must have feature with documents to be protected from unauthorized encryption or modification.

1.39 The proposed solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.

1.40 The proposed solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source/Destination/ Port/Protocol/Application to provide stateful inspection and high performance network virus scanning.

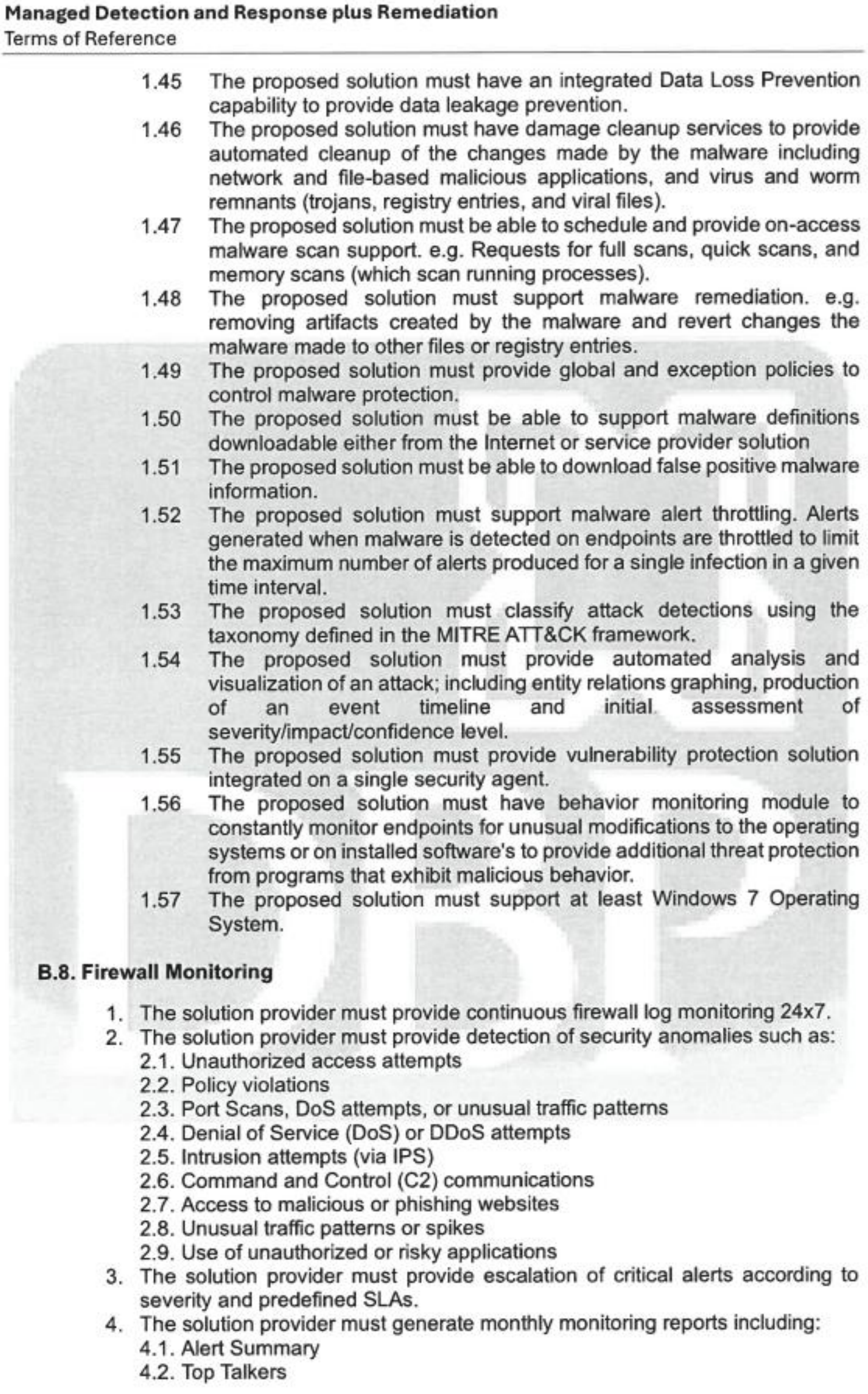
1.41 The proposed solution must have an integrated Application Control to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities.

1.42 The proposed Application Control solution must provide global and local real-time threat intelligence based on good file reputation data correlated across a global network.

1.43 The proposed Device Control solution must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The devices able to be restricted must include but not limited to the following:

i. USB Storage Drives (Also able to disable autorun)
ii. CD-ROM
iii. Floppy Disk
iv. Network Drives

1.44 The proposed Device Control solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT , Imaging Devices, Wireless Nic, Infrared devices



1.45 The proposed solution must have an integrated Data Loss Prevention capability to provide data leakage prevention.

1.46 The proposed solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (trojans, registry entries, and viral files).

1.47 The proposed solution must be able to schedule and provide on-access malware scan support. e.g. Requests for full scans, quick scans, and memory scans (which scan running processes).

1.48 The proposed solution must support malware remediation. e.g. removing artifacts created by the malware and revert changes the malware made to other files or registry entries.

1.49 The proposed solution must provide global and exception policies to control malware protection.

1.50 The proposed solution must be able to support malware definitions downloadable either from the Internet or service provider solution

1.51 The proposed solution must be able to download false positive malware information.

1.52 The proposed solution must support malware alert throttling. Alerts generated when malware is detected on endpoints are throttled to limit the maximum number of alerts produced for a single infection in a given time interval.

1.53 The proposed solution must classify attack detections using the taxonomy defined in the MITRE ATT&CK framework.

1.54 The proposed solution must provide automated analysis and visualization of an attack; including entity relations graphing, production of an event timeline and initial assessment of severity/impact/confidence level.

1.55 The proposed solution must provide vulnerability protection solution integrated on a single security agent.

1.56 The proposed solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.

1.57 The proposed solution must support at least Windows 7 Operating System.

B.8. Firewall Monitoring

1. The solution provider must provide continuous firewall log monitoring 24x7.
2. The solution provider must provide detection of security anomalies such as:
   2.1. Unauthorized access attempts
   2.2. Policy violations
   2.3. Port Scans, DoS attempts, or unusual traffic patterns
   2.4. Denial of Service (DoS) or DDoS attempts
   2.5. Intrusion attempts (via IPS)
   2.6. Command and Control (C2) communications
   2.7. Access to malicious or phishing websites
   2.8. Unusual traffic patterns or spikes
   2.9. Use of unauthorized or risky applications
3. The solution provider must provide escalation of critical alerts according to severity and predefined SLAs.
4. The solution provider must generate monthly monitoring reports including:
   4.1. Alert Summary
   4.2. Top Talkers

4.3. Policy usage
4.4. Threat trends

B.9. CSOC Facility Layout

Technical Specifications	Quantity
1. Videowall 2 x 3 Display, Diagonal Size 55", Resolution 1920x1080 (min), with wall-mounting brackets.	6 units
2. Videowall Controller (Minimum Core i9 12th Gen) and Videowall Management Software	1 unit
3. Triple Monitor Workstation with table console, chair and peripherals.	3 sets
4. Uninterruptible Power Supply (UPS) covering the power load requirements of the CSOC equipment.	1 lot
5. Air Cooling Unit (ACU) covering the CSOC area	1 lot
6. Networks (42u Modular Rack, 24port POE Switch, cablings, roughing in materials and accessories).	1 lot
7. Other Miscellaneous Components (video capture card, graphic card, HDMI extender/splitter, USB extender, wall plate, etc.)	1 lot
8. Installation, Configuration and Knowledge Transfer.	1 lot

IV. PERIOD COVERAGE

The contract of the project shall cover the delivery, subscription, installation, configuration, testing and commissioning including training, maintenance and after Sales Support. Which will commence upon receipt of the ***Notice to Proceed*** by the bidder. License subscription will start upon issuance of the Certificate Acceptance by DBP.

V. IMPLEMENTATION DELIVERABLES

The selected service provider shall provide 3 years subscription of Cloud Based Email Security for 5,000 mailbox, 5500 sensors of Endpoint Detection and Response (EDR), Endpoint Protection (workstation)for 4,750 endpoints and on-premise EDR solution for 750 Servers, 2 units of on-premise Network Forensics/ Packet Capture Solution, 1 unit of Network Intrusion Prevention System (IPS) with 3 years maintenance support, Security awareness license for 500 users and 1 lot Cyber Security Operation Center (CSOC) Facility Layout (Section III under B.8).

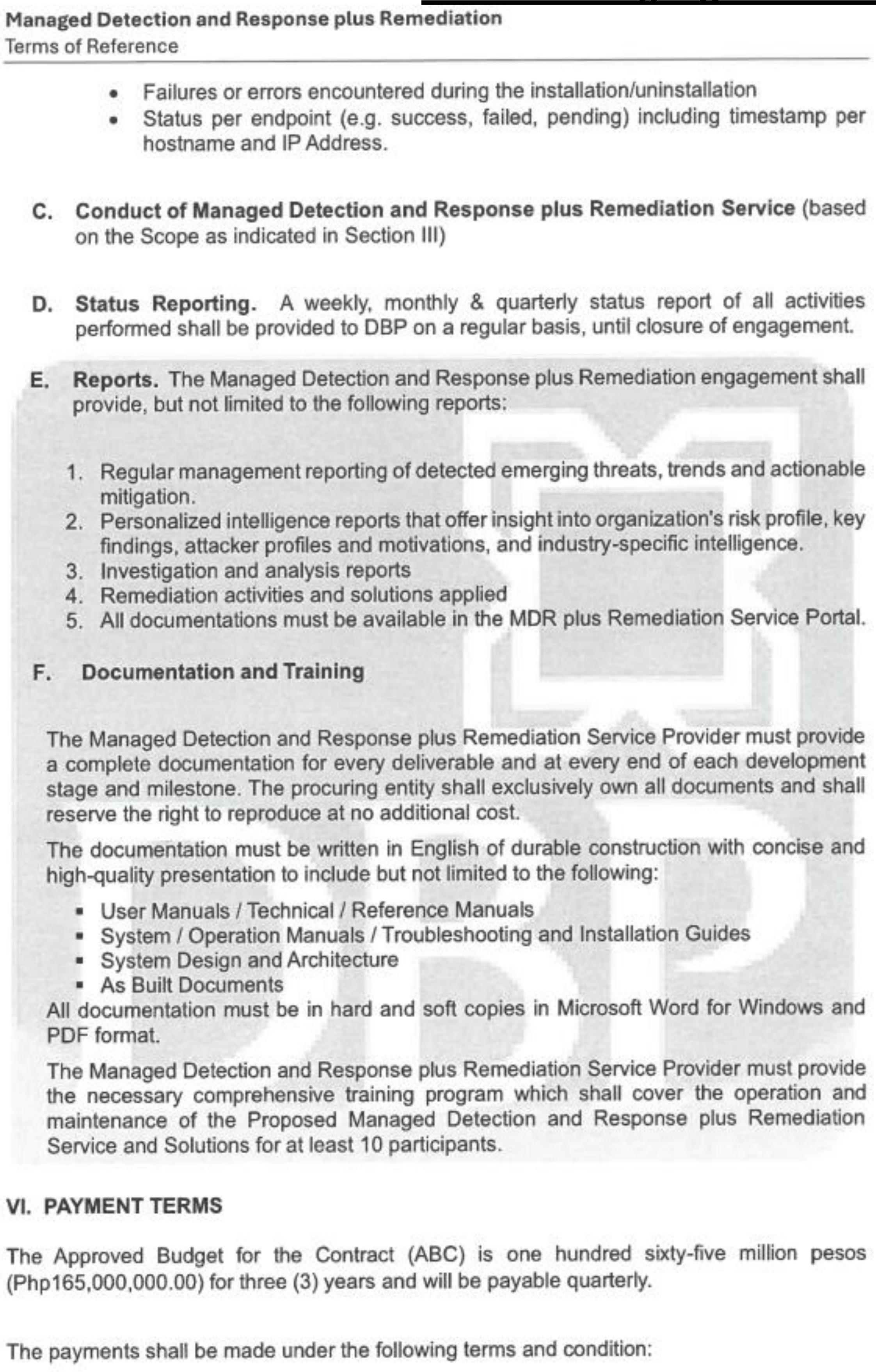
A. Work Plan. This must contain, at a minimum, the following:

1. Scope
2. Breakdown of regular activities for Manage Detection and Response plus Remediation
3. Deliverables

B. Technology Deployment. All required endpoint and network technology shall remain fully operational throughout the engagement period. The deployment and disposition of these technologies shall be carried out by the Service Provider, under the monitoring of DBP. Additionally, the Service Provider must utilize a reliable tool for deploying and un-installing the agent.

The Service Provider must provide weekly status report with the following details:

- Number of successful and unsuccessful endpoints installation.



- Failures or errors encountered during the installation/uninstallation
- Status per endpoint (e.g. success, failed, pending) including timestamp per hostname and IP Address.

C. **Conduct of Managed Detection and Response plus Remediation Service** (based on the Scope as indicated in Section III)

D. **Status Reporting.** A weekly, monthly & quarterly status report of all activities performed shall be provided to DBP on a regular basis, until closure of engagement.

E. **Reports.** The Managed Detection and Response plus Remediation engagement shall provide, but not limited to the following reports:

1. Regular management reporting of detected emerging threats, trends and actionable mitigation.
2. Personalized intelligence reports that offer insight into organization's risk profile, key findings, attacker profiles and motivations, and industry-specific intelligence.
3. Investigation and analysis reports
4. Remediation activities and solutions applied
5. All documentations must be available in the MDR plus Remediation Service Portal.

F. **Documentation and Training**

The Managed Detection and Response plus Remediation Service Provider must provide a complete documentation for every deliverable and at every end of each development stage and milestone. The procuring entity shall exclusively own all documents and shall reserve the right to reproduce at no additional cost.

The documentation must be written in English of durable construction with concise and high-quality presentation to include but not limited to the following:

- User Manuals / Technical / Reference Manuals
- System / Operation Manuals / Troubleshooting and Installation Guides
- System Design and Architecture
- As Built Documents

All documentation must be in hard and soft copies in Microsoft Word for Windows and PDF format.

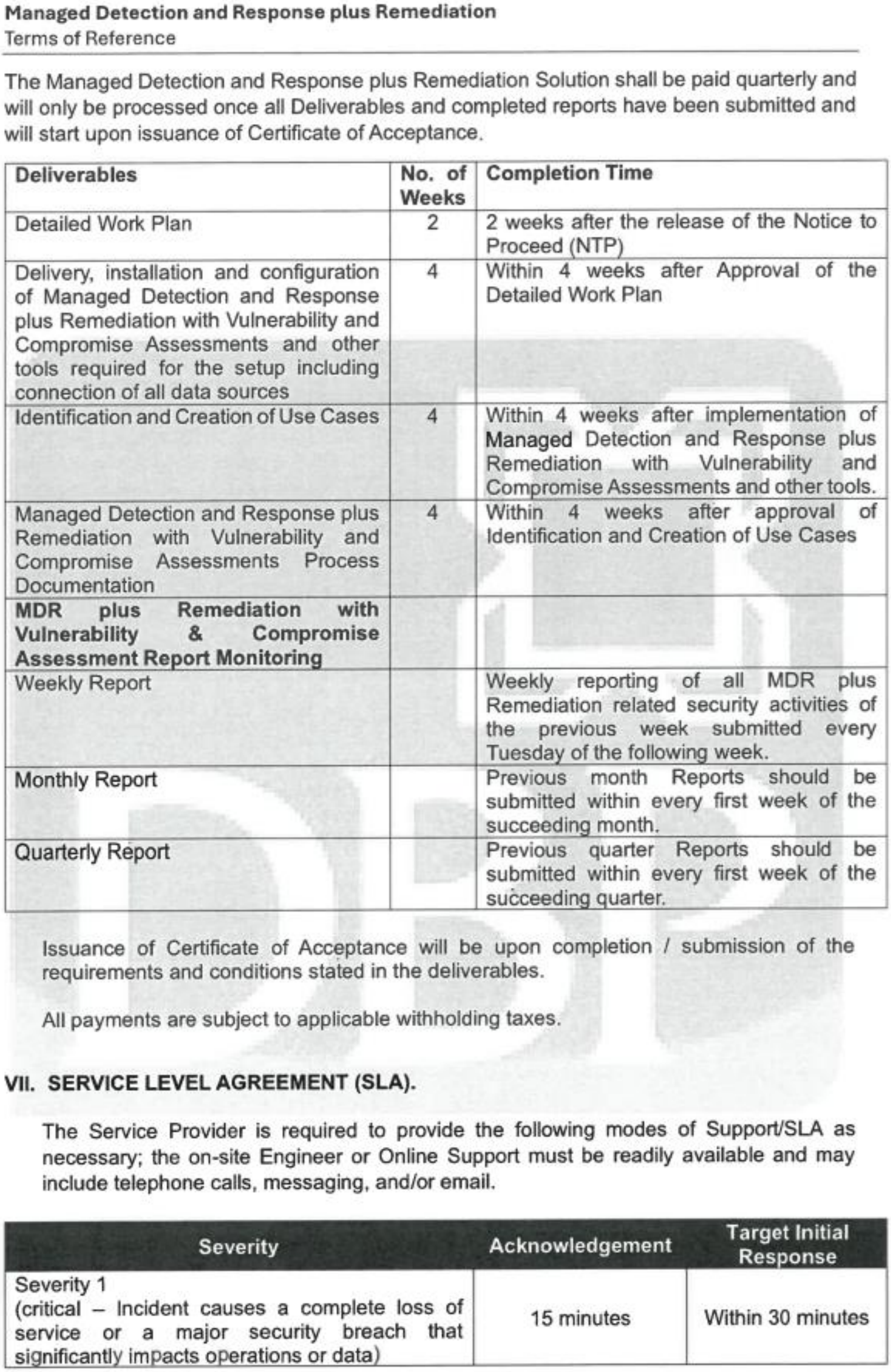
The Managed Detection and Response plus Remediation Service Provider must provide the necessary comprehensive training program which shall cover the operation and maintenance of the Proposed Managed Detection and Response plus Remediation Service and Solutions for at least 10 participants.

VI. PAYMENT TERMS

The Approved Budget for the Contract (ABC) is one hundred sixty-five million pesos (Php165,000,000.00) for three (3) years and will be payable quarterly.

The payments shall be made under the following terms and condition:

FORM 9-A (page 23 of 29)



The Managed Detection and Response plus Remediation Solution shall be paid quarterly and will only be processed once all Deliverables and completed reports have been submitted and will start upon issuance of Certificate of Acceptance.

Deliverables	No. of Weeks	Completion Time
Detailed Work Plan	2	2 weeks after the release of the Notice to Proceed (NTP)
Delivery, installation and configuration of Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments and other tools required for the setup including connection of all data sources	4	Within 4 weeks after Approval of the Detailed Work Plan
Identification and Creation of Use Cases	4	Within 4 weeks after implementation of Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments and other tools.
Managed Detection and Response plus Remediation with Vulnerability and Compromise Assessments Process Documentation	4	Within 4 weeks after approval of Identification and Creation of Use Cases
MDR plus Remediation with Vulnerability & Compromise Assessment Report Monitoring		
Weekly Report		Weekly reporting of all MDR plus Remediation related security activities of the previous week submitted every Tuesday of the following week.
Monthly Report		Previous month Reports should be submitted within every first week of the succeeding month.
Quarterly Report		Previous quarter Reports should be submitted within every first week of the succeeding quarter.

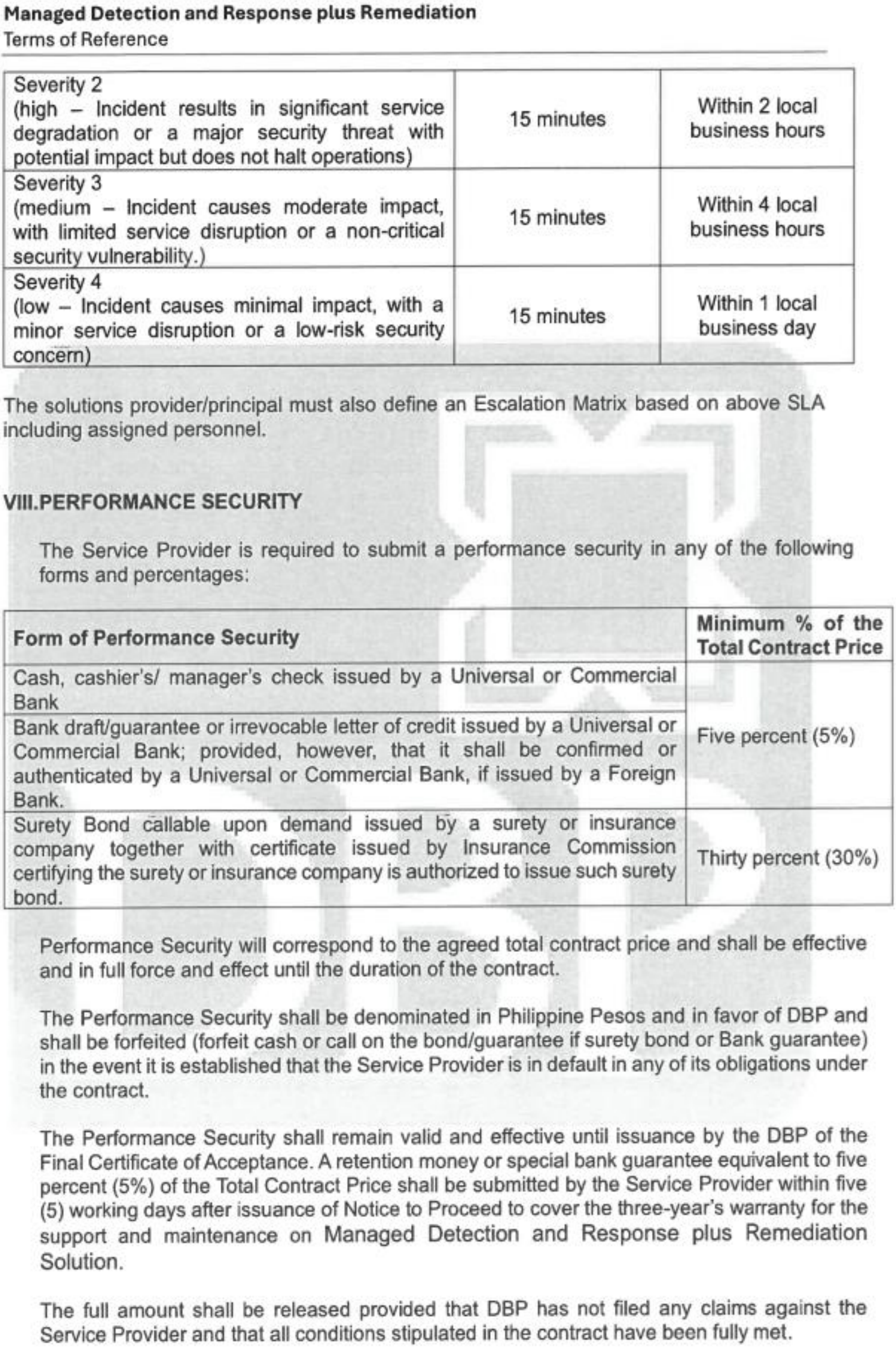
Issuance of Certificate of Acceptance will be upon completion / submission of the requirements and conditions stated in the deliverables.

All payments are subject to applicable withholding taxes.

VII. SERVICE LEVEL AGREEMENT (SLA).

The Service Provider is required to provide the following modes of Support/SLA as necessary; the on-site Engineer or Online Support must be readily available and may include telephone calls, messaging, and/or email.

Severity	Acknowledgement	Target Initial Response
Severity 1 (critical – Incident causes a complete loss of service or a major security breach that significantly impacts operations or data)	15 minutes	Within 30 minutes



Severity 2 (high – Incident results in significant service degradation or a major security threat with potential impact but does not halt operations)	15 minutes	Within 2 local business hours
Severity 3 (medium – Incident causes moderate impact, with limited service disruption or a non-critical security vulnerability.)	15 minutes	Within 4 local business hours
Severity 4 (low – Incident causes minimal impact, with a minor service disruption or a low-risk security concern)	15 minutes	Within 1 local business day

The solutions provider/principal must also define an Escalation Matrix based on above SLA including assigned personnel.

VIII.PERFORMANCE SECURITY

The Service Provider is required to submit a performance security in any of the following forms and percentages:

Form of Performance Security	Minimum % of the Total Contract Price
Cash, cashier's/ manager's check issued by a Universal or Commercial Bank	Five percent (5%)
Bank draft/guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; provided, however, that it shall be confirmed or authenticated by a Universal or Commercial Bank, if issued by a Foreign Bank.	
Surety Bond callable upon demand issued by a surety or insurance company together with certificate issued by Insurance Commission certifying the surety or insurance company is authorized to issue such surety bond.	Thirty percent (30%)

Performance Security will correspond to the agreed total contract price and shall be effective and in full force and effect until the duration of the contract.

The Performance Security shall be denominated in Philippine Pesos and in favor of DBP and shall be forfeited (forfeit cash or call on the bond/guarantee if surety bond or Bank guarantee) in the event it is established that the Service Provider is in default in any of its obligations under the contract.

The Performance Security shall remain valid and effective until issuance by the DBP of the Final Certificate of Acceptance. A retention money or special bank guarantee equivalent to five percent (5%) of the Total Contract Price shall be submitted by the Service Provider within five (5) working days after issuance of Notice to Proceed to cover the three-year's warranty for the support and maintenance on Managed Detection and Response plus Remediation Solution.

The full amount shall be released provided that DBP has not filed any claims against the Service Provider and that all conditions stipulated in the contract have been fully met.

The Service Provider shall extend the validity of the Performance Security in the event of extension of the contract.

IX. BIDDING REQUIREMENTS

Documents required for the Bid Opening:

1. Statement of completed contract of a similar nature within the past five (5) years, from the date of submission and receipt of bids, either a single contract similar to the project equivalent to at least 50% of the ABC, or at least two (2) similar contract, the sum of which must at least be equivalent to 50% of the ABC, provided the largest of these similar contracts must be at least 25% of the ABC. A similar contract refers to any Cybersecurity Managed Services solution includes the delivery, subscription, installation, and/or maintenance and support.

2. The solutions provider must be an authorized partner/reseller of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.

3. Accomplished Annex A: Summary of Technical Compliance for the proposed solution, ensuring it is cross-referenced with all of DBP's terms of reference, duly signed by the bidder's authorized representative.

4. The solutions provider must be an authorized partner of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.

5. The solutions provider/principal must comply with the following industry certifications and standards at a minimum.

   - ISO 27001 (Information Security Management Systems)
   - ISO 27014 (Governance and Information Security)
   - ISO 27034 (Application Security),
   - System and Organization Controls (SOC) 2
   - System and Organization Controls (SOC) 3
   - Payment Card Industry Data Security Standard (PCI DSS).

X. NON-DISCLOSURE CONDITION

The winning Bidder shall strictly adhere to the confidentiality agreement with the Bank. Information about DBP and its operation in this document is considered proprietary and confidential and must be treated as such by the recipients of this Technical Specifications. In the same manner, the responses to the Technical Specification which shall be specified as confidential shall not be disclosed to any third party.

1. Each party agrees to hold and maintain confidential all materials and information which shall come into its possession or knowledge in connection with the project or its performance, and not to make use hereof other than for the purpose of this project.

2. After completion of the project, all materials, data, proprietary information and other related documents provided to the winning bidder, and which are hereby deemed owned by DBP shall be returned to DBP.

3. The winning bidder undertake that it shall make appropriate instructions to its employees who need to have access to such information and materials to satisfy and comply with its confidential obligation as set forth in this Section.

4. This confidentiality obligation shall survive even after the termination of the contract.

5. The winning bidder shall, likewise, oblige the provider to be bound by this confidentiality contract.

6. The winning bidder's breach of this confidentiality provision shall entitle DBP to legal and other equitable remedies including but not limited to the immediate cancellation of the contract and shall entitle DBP for claim for damages and injunctive relief under the circumstances. DBP may also elect to terminate further access by the winning bidder to any data and information.

7. A Non-Disclosure Agreement between DBP and the winning bidder will form part of the contract that outlines confidential material, knowledge, or information that both parties wish to share with one another for certain purposes but wish to restrict access for or by third parties.

XI. POST QUALIFICATION REQUIREMENTS

The bidder shall be required to demonstrate the proposed MDR+R solution, in reference to the Bidders compliance to Section III – Scope of Work, within ten (10) calendar days after receipt of the Notice of Lowest/Single Calculated Bid.

XII. LIQUIDATED DAMAGES

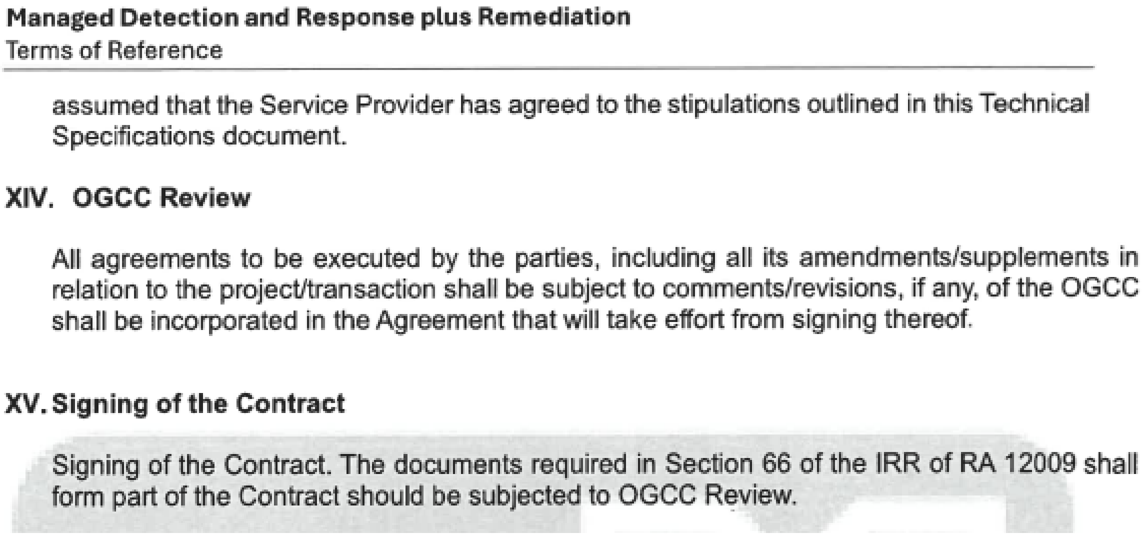
In case the Service Provider is unable to comply with the terms and conditions of this Agreement or fails to satisfactorily deliver the Solution or part of the solution on time inclusive of the duly granted time extension, if any, DBP shall, without prejudice to its other remedies under this Agreement and under the applicable law, deduct from the Contract Price, as liquidated damages, the applicable rate of one tenth (1/10) of one (1) percent of the cost of the unperformed portion for every day of delay until actual delivery or performance.

Such amount shall be deducted from any money due such as stated in Performance Security Section IX, or which may become due to the Service Provider, or collected from any securities or warranties posted by the Service Provider, whichever is convenient to DBP.

In case the total sum of liquidated damages reaches ten percent (10%) of the total contract price, DBP may rescind or terminate the Agreement, without prejudice to other courses of action and remedies open to it.

XIII. Signing of the Contract

The necessary documents as per the 2016 Revised Implementing Rules and Regulations (RIRR) of Republic Act (RA) No. 9184 are to be included as part of the Contract. It is



assumed that the Service Provider has agreed to the stipulations outlined in this Technical Specifications document.

XIV. OGCC Review

All agreements to be executed by the parties, including all its amendments/supplements in relation to the project/transaction shall be subject to comments/revisions, if any, of the OGCC shall be incorporated in the Agreement that will take effort from signing thereof.

XV. Signing of the Contract

Signing of the Contract. The documents required in Section 66 of the IRR of RA 12009 shall form part of the Contract should be subjected to OGCC Review.

FORM 9-A (page 28 of 29)

Managed Detection and Response plus Remediation
Terms of Reference

Figure 1

PROPOSED MDR+R CSOC NETWORK DIAGRAM

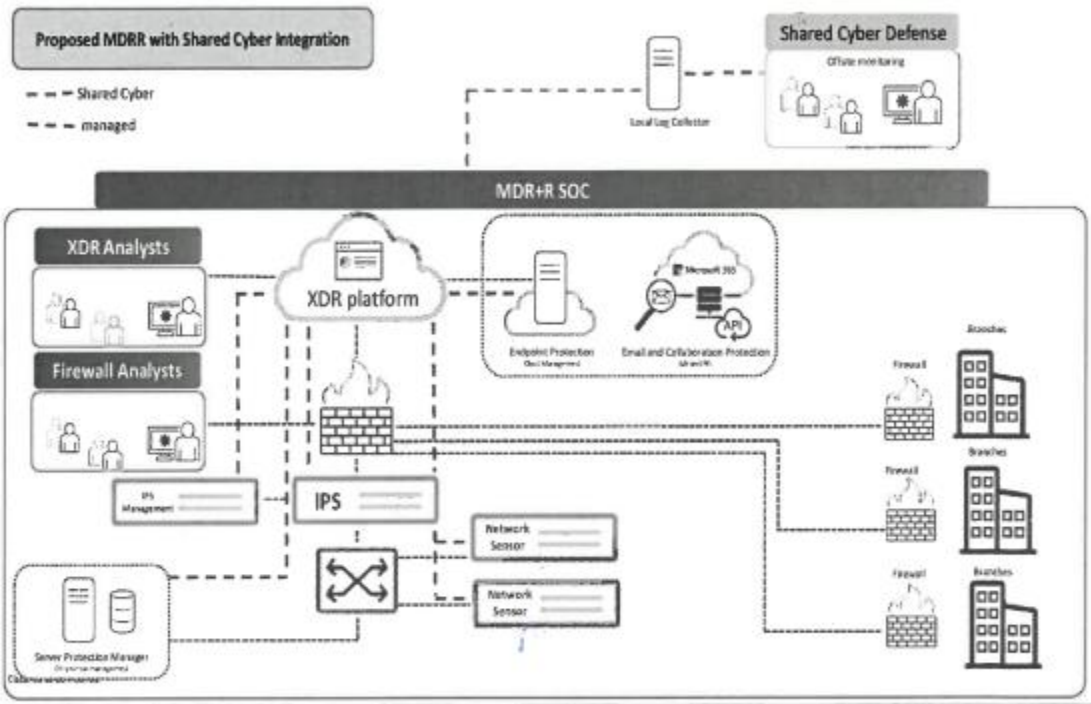
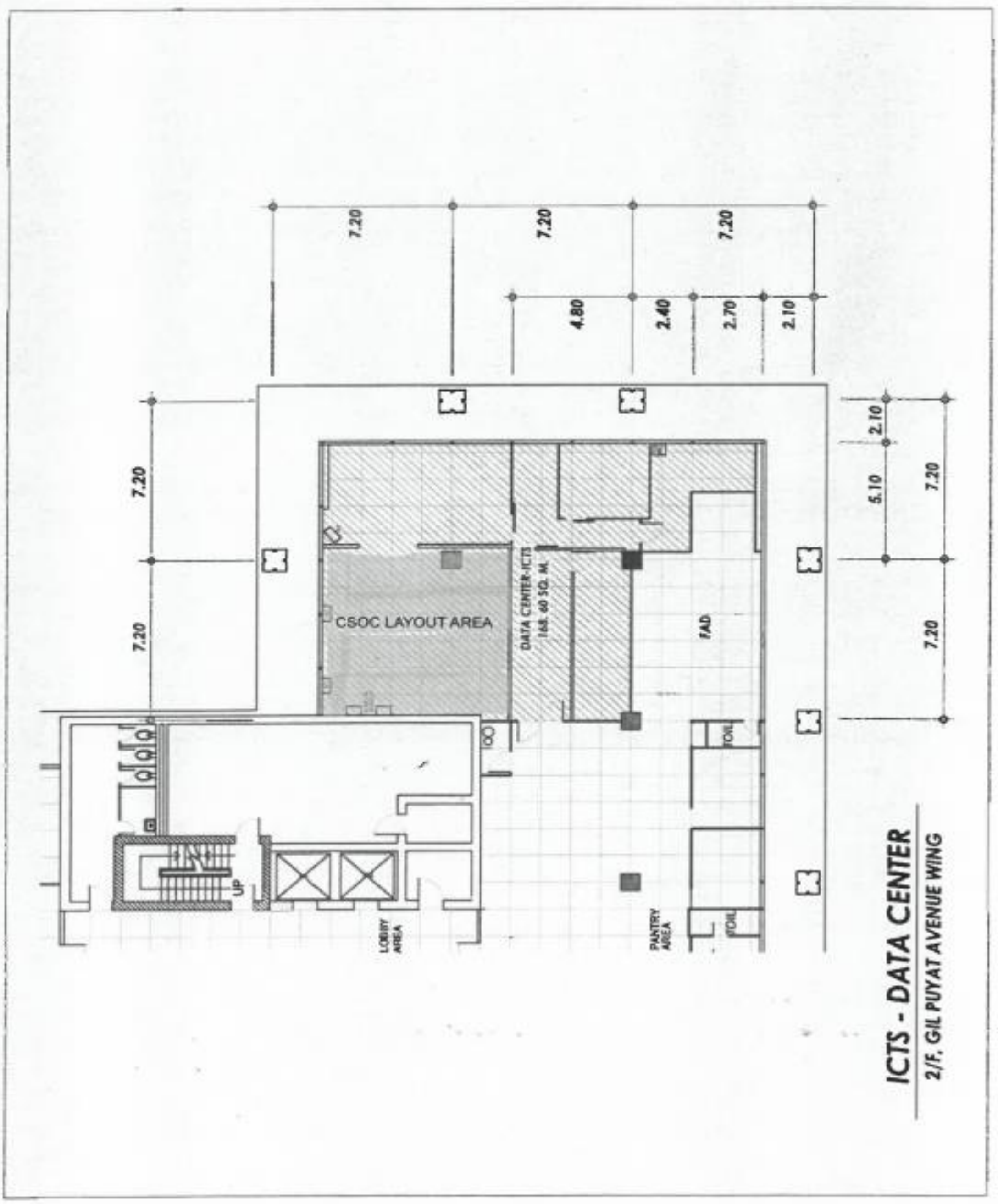
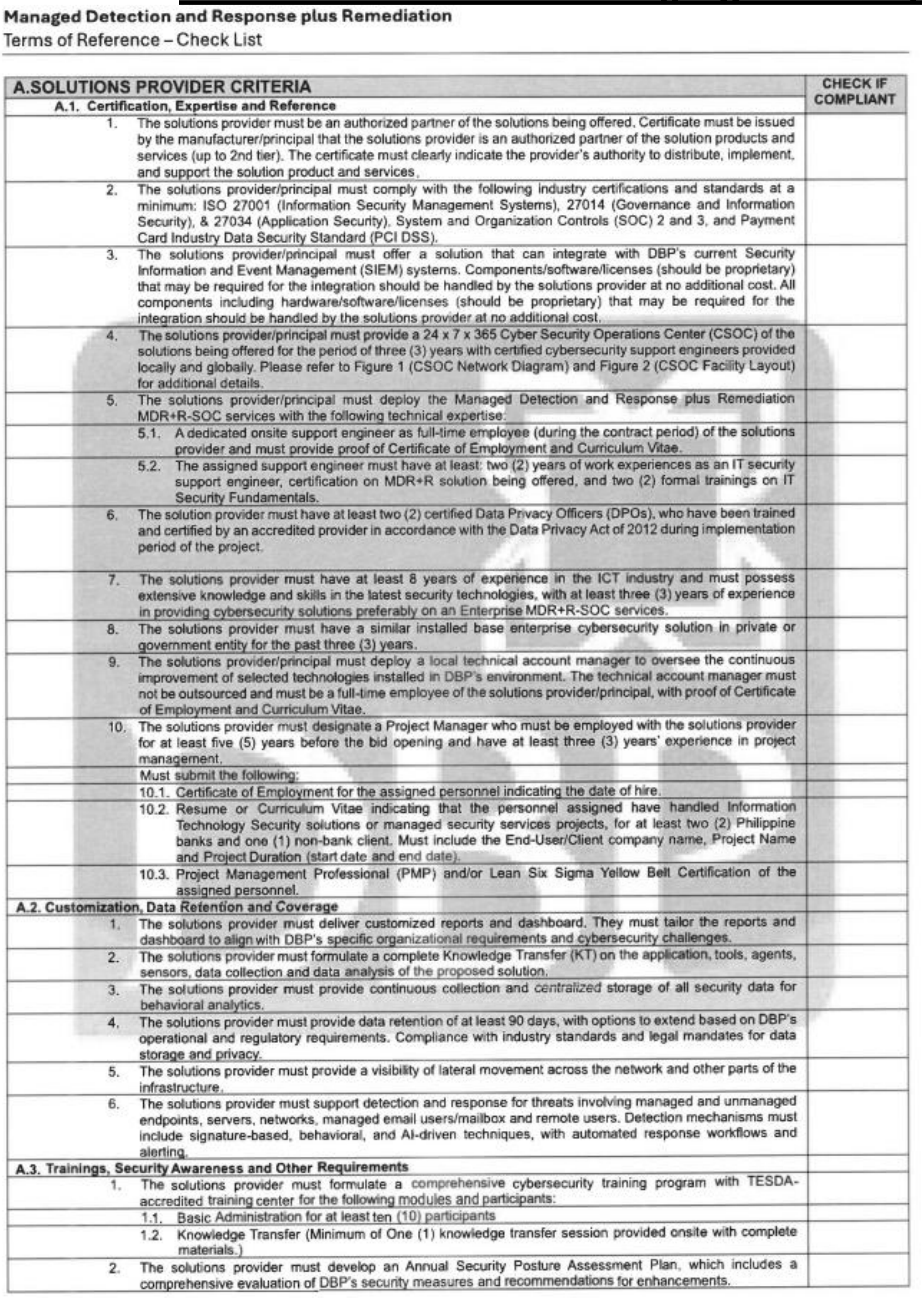


Figure 2

PROPOSED CSOC LAYOUT AREA



ANNEX A OF FORM 9-A (page 1 of 11)

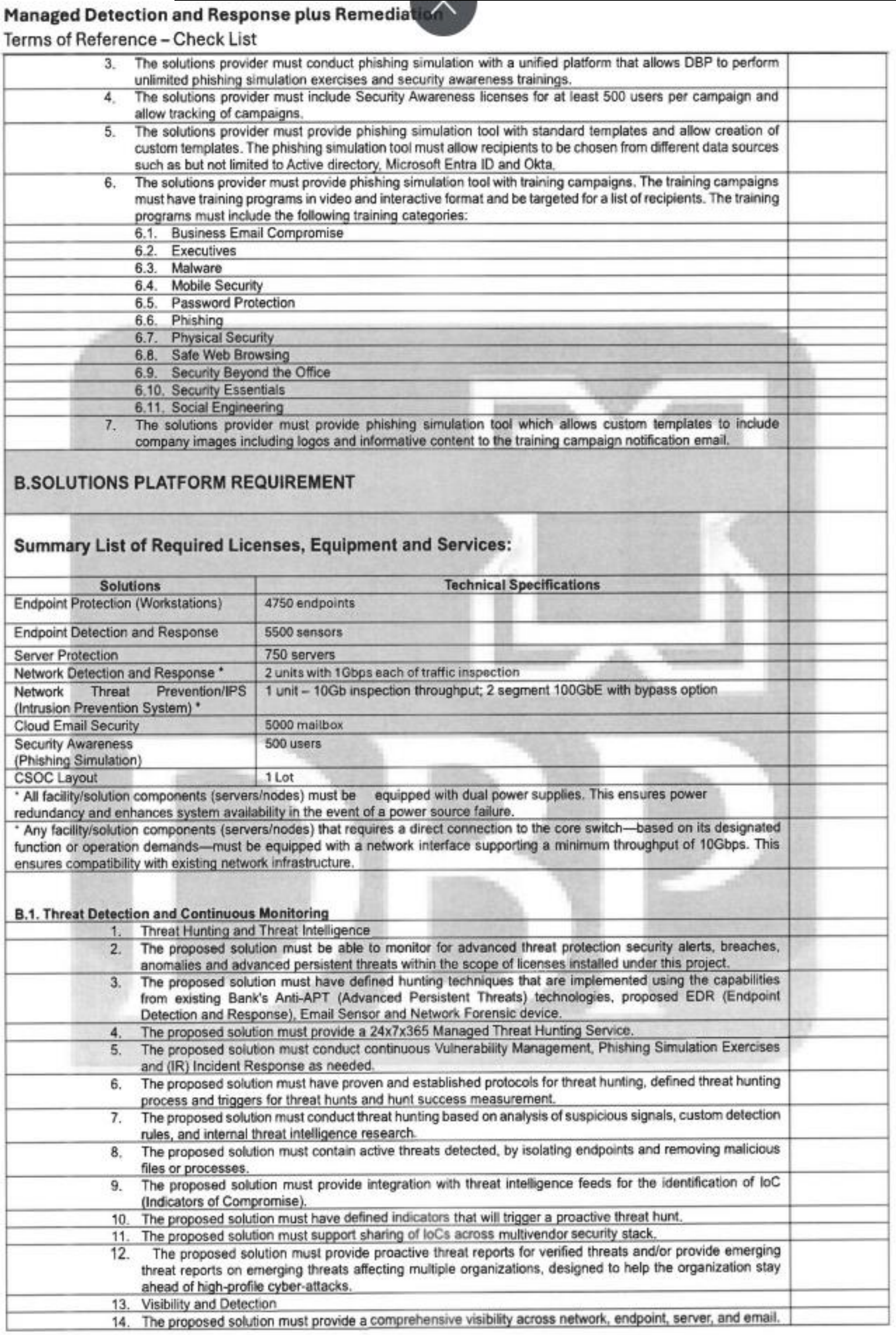


Managed Detection and Response plus Remediation

Terms of Reference – Check List

A.SOLUTIONS PROVIDER CRITERIA		CHECK IF COMPLIANT
A.1. Certification, Expertise and Reference		
1.	The solutions provider must be an authorized partner of the solutions being offered. Certificate must be issued by the manufacturer/principal that the solutions provider is an authorized partner of the solution products and services (up to 2nd tier). The certificate must clearly indicate the provider's authority to distribute, implement, and support the solution product and services.	
2.	The solutions provider/principal must comply with the following industry certifications and standards at a minimum: ISO 27001 (Information Security Management Systems), 27014 (Governance and Information Security), & 27034 (Application Security), System and Organization Controls (SOC) 2 and 3, and Payment Card Industry Data Security Standard (PCI DSS).	
3.	The solutions provider/principal must offer a solution that can integrate with DBP's current Security Information and Event Management (SIEM) systems. Components/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost. All components including hardware/software/licenses (should be proprietary) that may be required for the integration should be handled by the solutions provider at no additional cost.	
4.	The solutions provider/principal must provide a 24 x 7 x 365 Cyber Security Operations Center (CSOC) of the solutions being offered for the period of three (3) years with certified cybersecurity support engineers provided locally and globally. Please refer to Figure 1 (CSOC Network Diagram) and Figure 2 (CSOC Facility Layout) for additional details.	
5.	The solutions provider/principal must deploy the Managed Detection and Response plus Remediation MDR+R-SOC services with the following technical expertise:	
	5.1. A dedicated onsite support engineer as full-time employee (during the contract period) of the solutions provider and must provide proof of Certificate of Employment and Curriculum Vitae.	
	5.2. The assigned support engineer must have at least: two (2) years of work experiences as an IT security support engineer, certification on MDR+R solution being offered, and two (2) formal trainings on IT Security Fundamentals.	
6.	The solution provider must have at least two (2) certified Data Privacy Officers (DPOs), who have been trained and certified by an accredited provider in accordance with the Data Privacy Act of 2012 during implementation period of the project.	
7.	The solutions provider must have at least 8 years of experience in the ICT industry and must possess extensive knowledge and skills in the latest security technologies, with at least three (3) years of experience in providing cybersecurity solutions preferably on an Enterprise MDR+R-SOC services.	
8.	The solutions provider must have a similar installed base enterprise cybersecurity solution in private or government entity for the past three (3) years.	
9.	The solutions provider/principal must deploy a local technical account manager to oversee the continuous improvement of selected technologies installed in DBP's environment. The technical account manager must not be outsourced and must be a full-time employee of the solutions provider/principal, with proof of Certificate of Employment and Curriculum Vitae.	
10.	The solutions provider must designate a Project Manager who must be employed with the solutions provider for at least five (5) years before the bid opening and have at least three (3) years' experience in project management.	
	Must submit the following:	
	10.1. Certificate of Employment for the assigned personnel indicating the date of hire.	
	10.2. Resume or Curriculum Vitae indicating that the personnel assigned have handled Information Technology Security solutions or managed security services projects, for at least two (2) Philippine banks and one (1) non-bank client. Must include the End-User/Client company name, Project Name and Project Duration (start date and end date).	
	10.3. Project Management Professional (PMP) and/or Lean Six Sigma Yellow Belt Certification of the assigned personnel.	
A.2. Customization, Data Retention and Coverage		
1.	The solutions provider must deliver customized reports and dashboard. They must tailor the reports and dashboard to align with DBP's specific organizational requirements and cybersecurity challenges.	
2.	The solutions provider must formulate a complete Knowledge Transfer (KT) on the application, tools, agents, sensors, data collection and data analysis of the proposed solution.	
3.	The solutions provider must provide continuous collection and *centralized* storage of all security data for behavioral analytics.	
4.	The solutions provider must provide data retention of at least 90 days, with options to extend based on DBP's operational and regulatory requirements. Compliance with industry standards and legal mandates for data storage and privacy.	
5.	The solutions provider must provide a visibility of lateral movement across the network and other parts of the infrastructure.	
6.	The solutions provider must support detection and response for threats involving managed and unmanaged endpoints, servers, networks, managed email users/mailbox and remote users. Detection mechanisms must include signature-based, behavioral, and AI-driven techniques, with automated response workflows and alerting.	
A.3. Trainings, Security Awareness and Other Requirements		
1.	The solutions provider must formulate a comprehensive cybersecurity training program with TESDA-accredited training center for the following modules and participants:	
	1.1. Basic Administration for at least ten (10) participants	
	1.2. Knowledge Transfer (Minimum of One (1) knowledge transfer session provided onsite with complete materials.)	
2.	The solutions provider must develop an Annual Security Posture Assessment Plan, which includes a comprehensive evaluation of DBP's security measures and recommendations for enhancements.	

ANNEX A OF FORM 9-A (page 2 of 11)



Managed Detection and Response plus Remediation

Terms of Reference – Check List

3. The solutions provider must conduct phishing simulation with a unified platform that allows DBP to perform unlimited phishing simulation exercises and security awareness trainings.
4. The solutions provider must include Security Awareness licenses for at least 500 users per campaign and allow tracking of campaigns.
5. The solutions provider must provide phishing simulation tool with standard templates and allow creation of custom templates. The phishing simulation tool must allow recipients to be chosen from different data sources such as but not limited to Active directory, Microsoft Entra ID and Okta.
6. The solutions provider must provide phishing simulation tool with training campaigns. The training campaigns must have training programs in video and interactive format and be targeted for a list of recipients. The training programs must include the following training categories:
   - 6.1. Business Email Compromise
   - 6.2. Executives
   - 6.3. Malware
   - 6.4. Mobile Security
   - 6.5. Password Protection
   - 6.6. Phishing
   - 6.7. Physical Security
   - 6.8. Safe Web Browsing
   - 6.9. Security Beyond the Office
   - 6.10. Security Essentials
   - 6.11. Social Engineering
7. The solutions provider must provide phishing simulation tool which allows custom templates to include company images including logos and informative content to the training campaign notification email.

B.SOLUTIONS PLATFORM REQUIREMENT

Summary List of Required Licenses, Equipment and Services:

Solutions	Technical Specifications
Endpoint Protection (Workstations)	4750 endpoints
Endpoint Detection and Response	5500 sensors
Server Protection	750 servers
Network Detection and Response *	2 units with 1Gbps each of traffic inspection
Network Threat Prevention/IPS (Intrusion Prevention System) *	1 unit – 10Gb inspection throughput; 2 segment 100GbE with bypass option
Cloud Email Security	5000 mailbox
Security Awareness (Phishing Simulation)	500 users
CSOC Layout	1 Lot

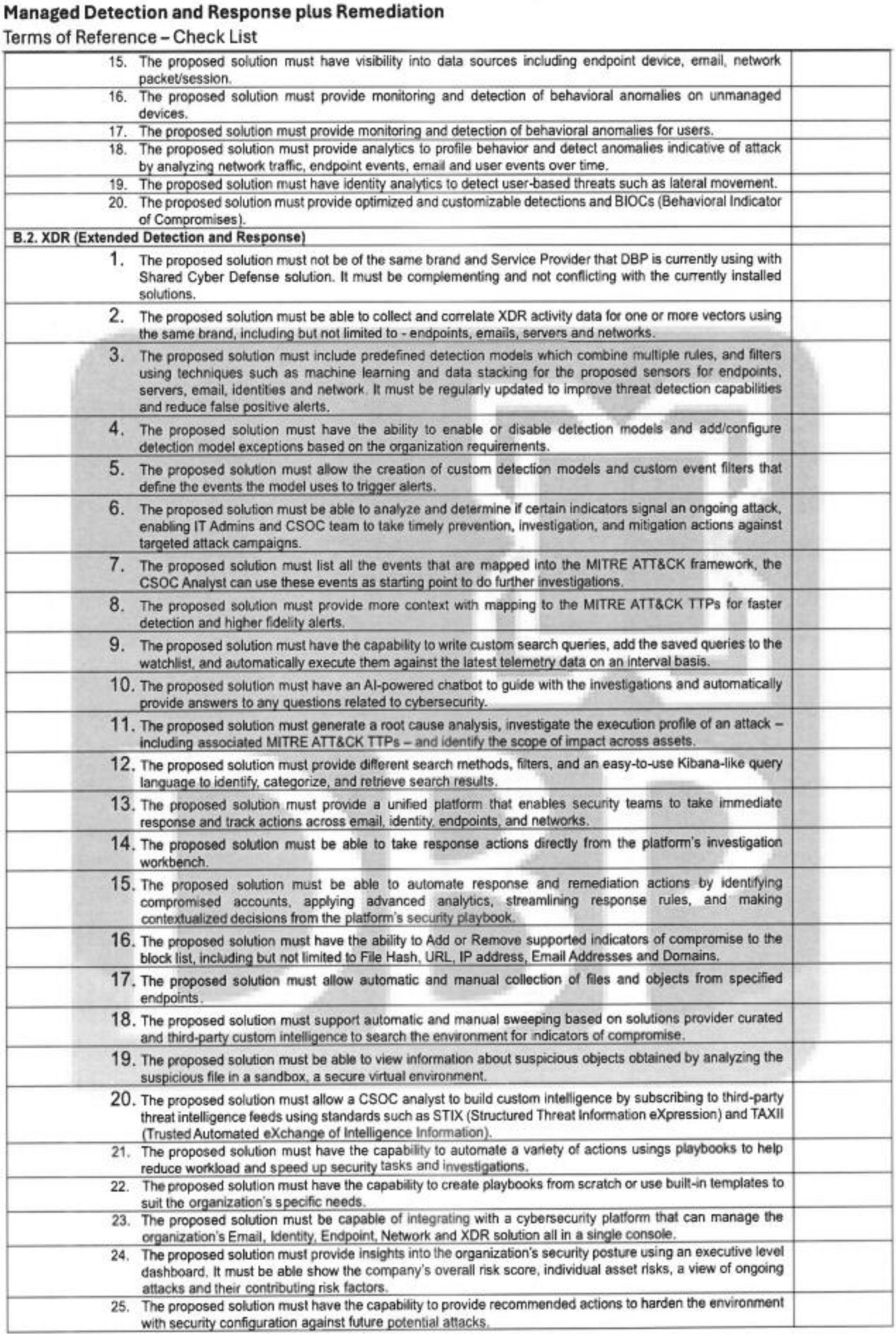
* All facility/solution components (servers/nodes) must be equipped with dual power supplies. This ensures power redundancy and enhances system availability in the event of a power source failure.

* Any facility/solution components (servers/nodes) that requires a direct connection to the core switch—based on its designated function or operation demands—must be equipped with a network interface supporting a minimum throughput of 10Gbps. This ensures compatibility with existing network infrastructure.

B.1. Threat Detection and Continuous Monitoring

1. Threat Hunting and Threat Intelligence
2. The proposed solution must be able to monitor for advanced threat protection security alerts, breaches, anomalies and advanced persistent threats within the scope of licenses installed under this project.
3. The proposed solution must have defined hunting techniques that are implemented using the capabilities from existing Bank's Anti-APT (Advanced Persistent Threats) technologies, proposed EDR (Endpoint Detection and Response), Email Sensor and Network Forensic device.
4. The proposed solution must provide a 24x7x365 Managed Threat Hunting Service.
5. The proposed solution must conduct continuous Vulnerability Management, Phishing Simulation Exercises and (IR) Incident Response as needed.
6. The proposed solution must have proven and established protocols for threat hunting, defined threat hunting process and triggers for threat hunts and hunt success measurement.
7. The proposed solution must conduct threat hunting based on analysis of suspicious signals, custom detection rules, and internal threat intelligence research.
8. The proposed solution must contain active threats detected, by isolating endpoints and removing malicious files or processes.
9. The proposed solution must provide integration with threat intelligence feeds for the identification of IoC (Indicators of Compromise).
10. The proposed solution must have defined indicators that will trigger a proactive threat hunt.
11. The proposed solution must support sharing of IoCs across multivendor security stack.
12. The proposed solution must provide proactive threat reports for verified threats and/or provide emerging threat reports on emerging threats affecting multiple organizations, designed to help the organization stay ahead of high-profile cyber-attacks.
13. Visibility and Detection
14. The proposed solution must provide a comprehensive visibility across network, endpoint, server, and email.

ANNEX A OF FORM 9-A (page 3 of 11)

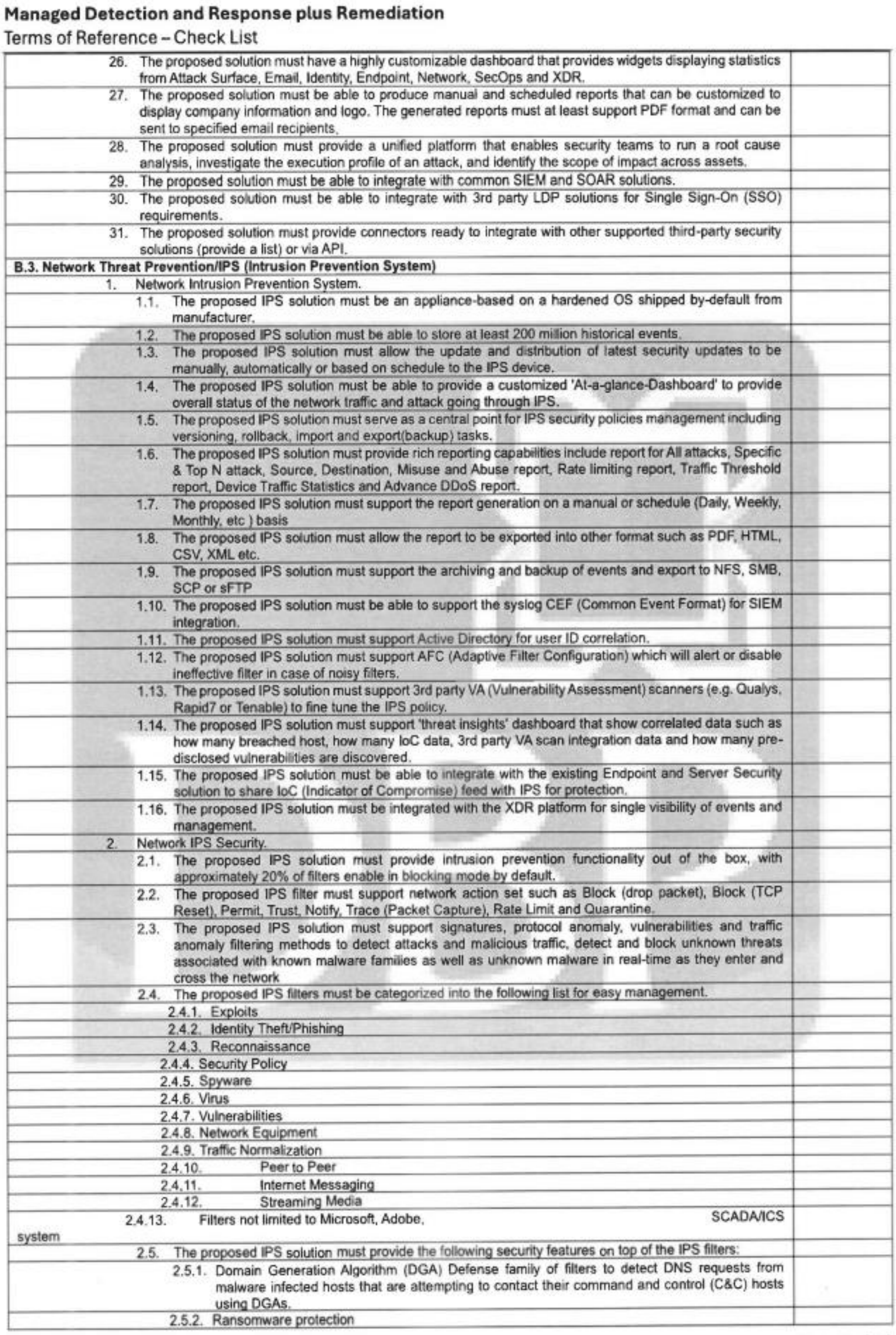


Managed Detection and Response plus Remediation

Terms of Reference – Check List

15. The proposed solution must have visibility into data sources including endpoint device, email, network packet/session.	
16. The proposed solution must provide monitoring and detection of behavioral anomalies on unmanaged devices.	
17. The proposed solution must provide monitoring and detection of behavioral anomalies for users.	
18. The proposed solution must provide analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, email and user events over time.	
19. The proposed solution must have identity analytics to detect user-based threats such as lateral movement.	
20. The proposed solution must provide optimized and customizable detections and BIOCs (Behavioral Indicator of Compromises).	
B.2. XDR (Extended Detection and Response)	
1. The proposed solution must not be of the same brand and Service Provider that DBP is currently using with Shared Cyber Defense solution. It must be complementing and not conflicting with the currently installed solutions.	
2. The proposed solution must be able to collect and correlate XDR activity data for one or more vectors using the same brand, including but not limited to - endpoints, emails, servers and networks.	
3. The proposed solution must include predefined detection models which combine multiple rules, and filters using techniques such as machine learning and data stacking for the proposed sensors for endpoints, servers, email, identities and network. It must be regularly updated to improve threat detection capabilities and reduce false positive alerts.	
4. The proposed solution must have the ability to enable or disable detection models and add/configure detection model exceptions based on the organization requirements.	
5. The proposed solution must allow the creation of custom detection models and custom event filters that define the events the model uses to trigger alerts.	
6. The proposed solution must be able to analyze and determine if certain indicators signal an ongoing attack, enabling IT Admins and CSOC team to take timely prevention, investigation, and mitigation actions against targeted attack campaigns.	
7. The proposed solution must list all the events that are mapped into the MITRE ATT&CK framework, the CSOC Analyst can use these events as starting point to do further investigations.	
8. The proposed solution must provide more context with mapping to the MITRE ATT&CK TTPs for faster detection and higher fidelity alerts.	
9. The proposed solution must have the capability to write custom search queries, add the saved queries to the watchlist, and automatically execute them against the latest telemetry data on an interval basis.	
10. The proposed solution must have an AI-powered chatbot to guide with the investigations and automatically provide answers to any questions related to cybersecurity.	
11. The proposed solution must generate a root cause analysis, investigate the execution profile of an attack – including associated MITRE ATT&CK TTPs – and identify the scope of impact across assets.	
12. The proposed solution must provide different search methods, filters, and an easy-to-use Kibana-like query language to identify, categorize, and retrieve search results.	
13. The proposed solution must provide a unified platform that enables security teams to take immediate response and track actions across email, identity, endpoints, and networks.	
14. The proposed solution must be able to take response actions directly from the platform's investigation workbench.	
15. The proposed solution must be able to automate response and remediation actions by identifying compromised accounts, applying advanced analytics, streamlining response rules, and making contextualized decisions from the platform's security playbook.	
16. The proposed solution must have the ability to Add or Remove supported indicators of compromise to the block list, including but not limited to File Hash, URL, IP address, Email Addresses and Domains.	
17. The proposed solution must allow automatic and manual collection of files and objects from specified endpoints.	
18. The proposed solution must support automatic and manual sweeping based on solutions provider curated and third-party custom intelligence to search the environment for indicators of compromise.	
19. The proposed solution must be able to view information about suspicious objects obtained by analyzing the suspicious file in a sandbox, a secure virtual environment.	
20. The proposed solution must allow a CSOC analyst to build custom intelligence by subscribing to third-party threat intelligence feeds using standards such as STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Intelligence Information).	
21. The proposed solution must have the capability to automate a variety of actions usings playbooks to help reduce workload and speed up security tasks and investigations.	
22. The proposed solution must have the capability to create playbooks from scratch or use built-in templates to suit the organization's specific needs.	
23. The proposed solution must be capable of integrating with a cybersecurity platform that can manage the organization's Email, Identity, Endpoint, Network and XDR solution all in a single console.	
24. The proposed solution must provide insights into the organization's security posture using an executive level dashboard. It must be able show the company's overall risk score, individual asset risks, a view of ongoing attacks and their contributing risk factors.	
25. The proposed solution must have the capability to provide recommended actions to harden the environment with security configuration against future potential attacks.	

ANNEX A OF FORM 9-A (page 4 of 11)

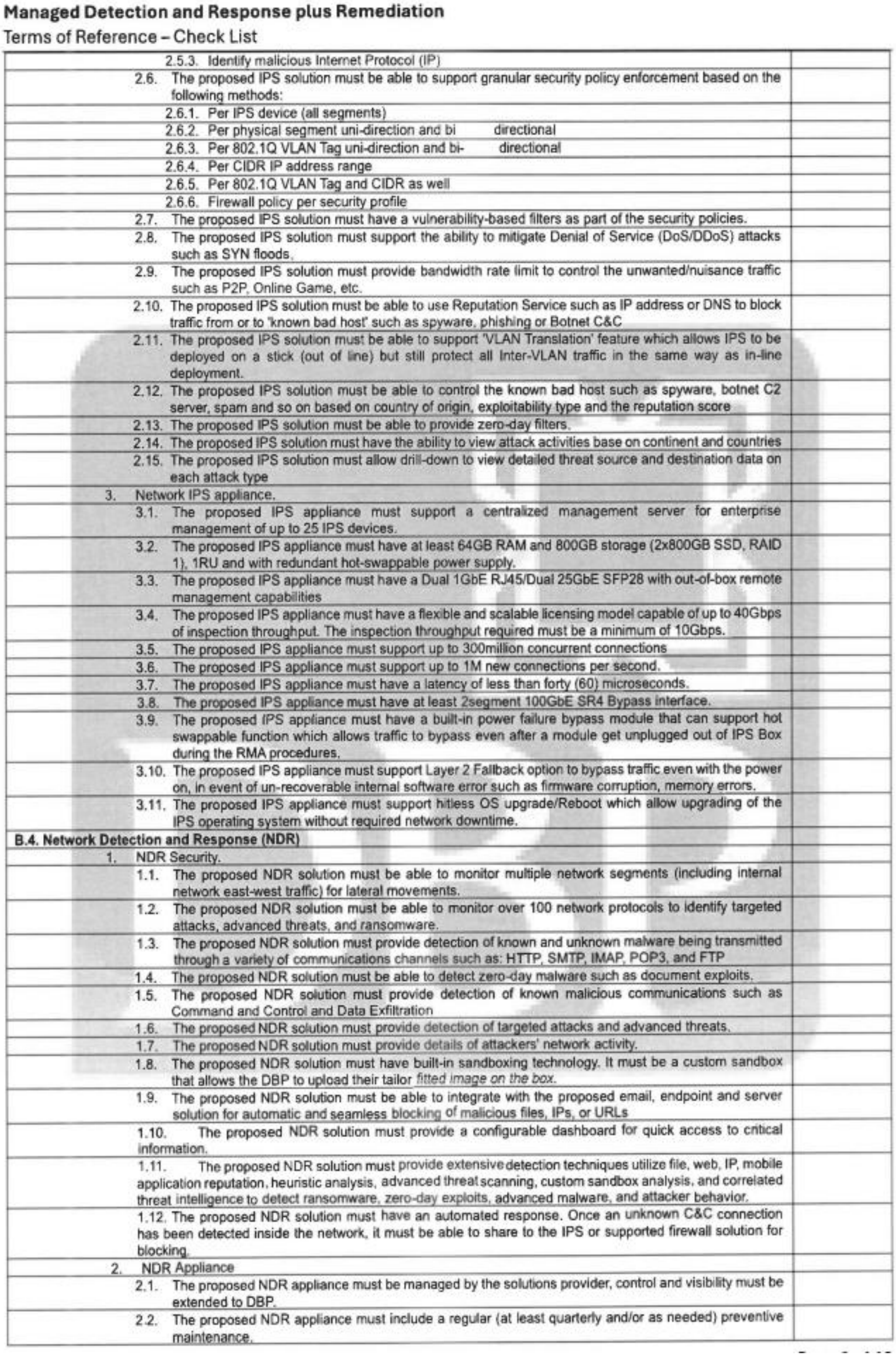


Managed Detection and Response plus Remediation

Terms of Reference – Check List

26. The proposed solution must have a highly customizable dashboard that provides widgets displaying statistics from Attack Surface, Email, Identity, Endpoint, Network, SecOps and XDR.	
27. The proposed solution must be able to produce manual and scheduled reports that can be customized to display company information and logo. The generated reports must at least support PDF format and can be sent to specified email recipients.	
28. The proposed solution must provide a unified platform that enables security teams to run a root cause analysis, investigate the execution profile of an attack, and identify the scope of impact across assets.	
29. The proposed solution must be able to integrate with common SIEM and SOAR solutions.	
30. The proposed solution must be able to integrate with 3rd party LDP solutions for Single Sign-On (SSO) requirements.	
31. The proposed solution must provide connectors ready to integrate with other supported third-party security solutions (provide a list) or via API.	
B.3. Network Threat Prevention/IPS (Intrusion Prevention System)	
1. Network Intrusion Prevention System.	
1.1. The proposed IPS solution must be an appliance-based on a hardened OS shipped by-default from manufacturer.	
1.2. The proposed IPS solution must be able to store at least 200 million historical events.	
1.3. The proposed IPS solution must allow the update and distribution of latest security updates to be manually, automatically or based on schedule to the IPS device.	
1.4. The proposed IPS solution must be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through IPS.	
1.5. The proposed IPS solution must serve as a central point for IPS security policies management including versioning, rollback, import and export(backup) tasks.	
1.6. The proposed IPS solution must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report.	
1.7. The proposed IPS solution must support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc) basis	
1.8. The proposed IPS solution must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.	
1.9. The proposed IPS solution must support the archiving and backup of events and export to NFS, SMB, SCP or sFTP	
1.10. The proposed IPS solution must be able to support the syslog CEF (Common Event Format) for SIEM integration.	
1.11. The proposed IPS solution must support Active Directory for user ID correlation.	
1.12. The proposed IPS solution must support AFC (Adaptive Filter Configuration) which will alert or disable ineffective filter in case of noisy filters.	
1.13. The proposed IPS solution must support 3rd party VA (Vulnerability Assessment) scanners (e.g. Qualys, Rapid7 or Tenable) to fine tune the IPS policy.	
1.14. The proposed IPS solution must support 'threat insights' dashboard that show correlated data such as how many breached host, how many IoC data, 3rd party VA scan integration data and how many pre-disclosed vulnerabilities are discovered.	
1.15. The proposed IPS solution must be able to integrate with the existing Endpoint and Server Security solution to share IoC (Indicator of Compromise) feed with IPS for protection.	
1.16. The proposed IPS solution must be integrated with the XDR platform for single visibility of events and management.	
2. Network IPS Security.	
2.1. The proposed IPS solution must provide intrusion prevention functionality out of the box, with approximately 20% of filters enable in blocking mode by default.	
2.2. The proposed IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine.	
2.3. The proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic, detect and block unknown threats associated with known malware families as well as unknown malware in real-time as they enter and cross the network	
2.4. The proposed IPS filters must be categorized into the following list for easy management.	
2.4.1. Exploits	
2.4.2. Identity Theft/Phishing	
2.4.3. Reconnaissance	
2.4.4. Security Policy	
2.4.5. Spyware	
2.4.6. Virus	
2.4.7. Vulnerabilities	
2.4.8. Network Equipment	
2.4.9. Traffic Normalization	
2.4.10. Peer to Peer	
2.4.11. Internet Messaging	
2.4.12. Streaming Media	
2.4.13. Filters not limited to Microsoft, Adobe, SCADA/ICS system	
2.5. The proposed IPS solution must provide the following security features on top of the IPS filters:	
2.5.1. Domain Generation Algorithm (DGA) Defense family of filters to detect DNS requests from malware infected hosts that are attempting to contact their command and control (C&C) hosts using DGAs.	
2.5.2. Ransomware protection	

ANNEX A OF FORM 9-A (page 5 of 11)

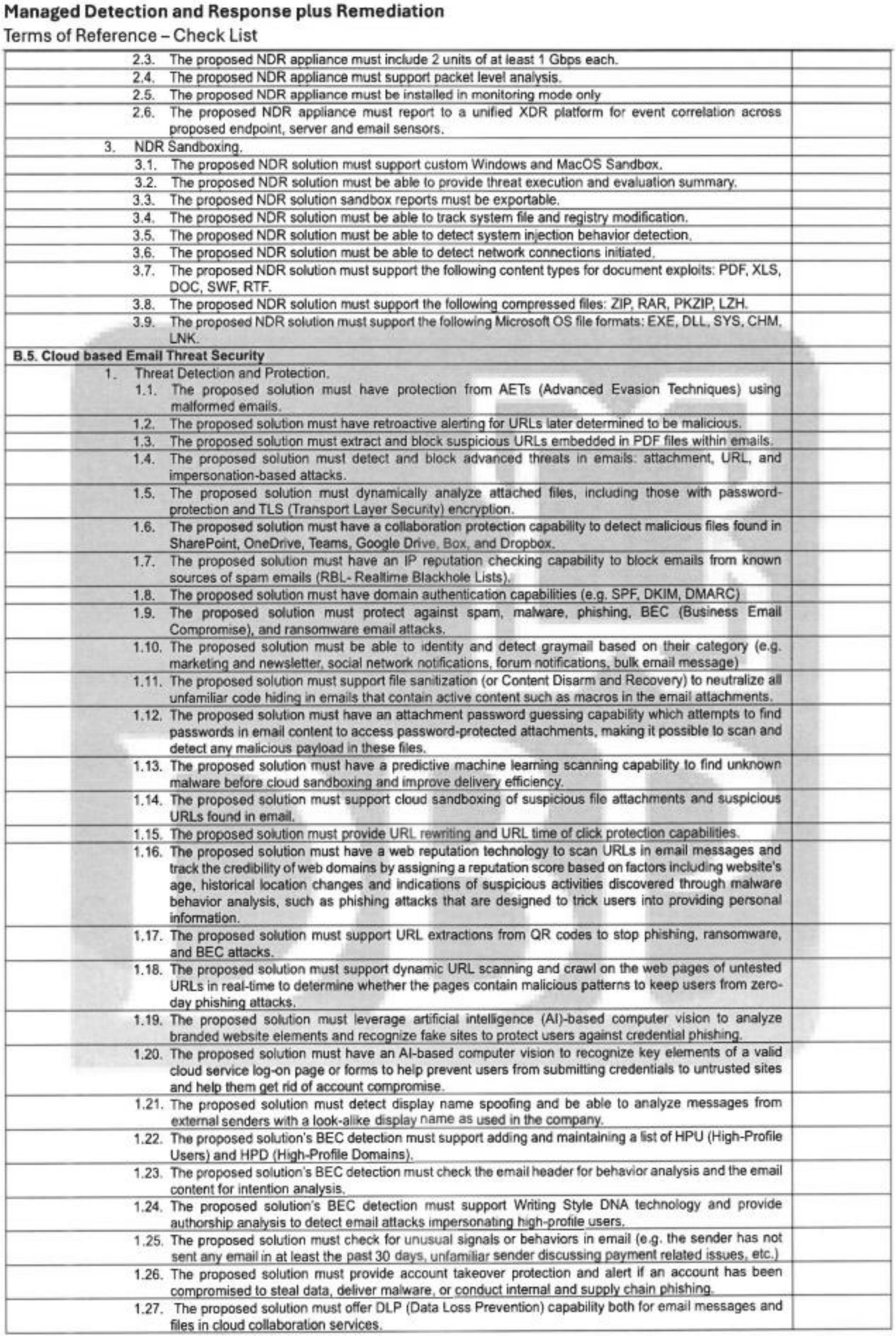


Managed Detection and Response plus Remediation

Terms of Reference – Check List

2.5.3. Identify malicious Internet Protocol (IP)	
2.6. The proposed IPS solution must be able to support granular security policy enforcement based on the following methods:	
2.6.1. Per IPS device (all segments)	
2.6.2. Per physical segment uni-direction and bi directional	
2.6.3. Per 802.1Q VLAN Tag uni-direction and bi- directional	
2.6.4. Per CIDR IP address range	
2.6.5. Per 802.1Q VLAN Tag and CIDR as well	
2.6.6. Firewall policy per security profile	
2.7. The proposed IPS solution must have a vulnerability-based filters as part of the security policies.	
2.8. The proposed IPS solution must support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods.	
2.9. The proposed IPS solution must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc.	
2.10. The proposed IPS solution must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C	
2.11. The proposed IPS solution must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment.	
2.12. The proposed IPS solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploitability type and the reputation score	
2.13. The proposed IPS solution must be able to provide zero-day filters.	
2.14. The proposed IPS solution must have the ability to view attack activities base on continent and countries	
2.15. The proposed IPS solution must allow drill-down to view detailed threat source and destination data on each attack type	
3. Network IPS appliance.	
3.1. The proposed IPS appliance must support a centralized management server for enterprise management of up to 25 IPS devices.	
3.2. The proposed IPS appliance must have at least 64GB RAM and 800GB storage (2x800GB SSD, RAID 1), 1RU and with redundant hot-swappable power supply.	
3.3. The proposed IPS appliance must have a Dual 1GbE RJ45/Dual 25GbE SFP28 with out-of-box remote management capabilities	
3.4. The proposed IPS appliance must have a flexible and scalable licensing model capable of up to 40Gbps of inspection throughput. The inspection throughput required must be a minimum of 10Gbps.	
3.5. The proposed IPS appliance must support up to 300million concurrent connections	
3.6. The proposed IPS appliance must support up to 1M new connections per second.	
3.7. The proposed IPS appliance must have a latency of less than forty (60) microseconds.	
3.8. The proposed IPS appliance must have at least 2segment 100GbE SR4 Bypass interface.	
3.9. The proposed IPS appliance must have a built-in power failure bypass module that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedures.	
3.10. The proposed IPS appliance must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors.	
3.11. The proposed IPS appliance must support hitless OS upgrade/Reboot which allow upgrading of the IPS operating system without required network downtime.	
B.4. Network Detection and Response (NDR)	
1. NDR Security.	
1.1. The proposed NDR solution must be able to monitor multiple network segments (including internal network east-west traffic) for lateral movements.	
1.2. The proposed NDR solution must be able to monitor over 100 network protocols to identify targeted attacks, advanced threats, and ransomware.	
1.3. The proposed NDR solution must provide detection of known and unknown malware being transmitted through a variety of communications channels such as: HTTP, SMTP, IMAP, POP3, and FTP	
1.4. The proposed NDR solution must be able to detect zero-day malware such as document exploits.	
1.5. The proposed NDR solution must provide detection of known malicious communications such as Command and Control and Data Exfiltration	
1.6. The proposed NDR solution must provide detection of targeted attacks and advanced threats.	
1.7. The proposed NDR solution must provide details of attackers' network activity.	
1.8. The proposed NDR solution must have built-in sandboxing technology. It must be a custom sandbox that allows the DBP to upload their tailor *fitted image on the box.*	
1.9. The proposed NDR solution must be able to integrate with the proposed email, endpoint and server solution for automatic and seamless blocking of malicious files, IPs, or URLs	
1.10. The proposed NDR solution must provide a configurable dashboard for quick access to critical information.	
1.11. The proposed NDR solution must provide extensive detection techniques utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.	
1.12. The proposed NDR solution must have an automated response. Once an unknown C&C connection has been detected inside the network, it must be able to share to the IPS or supported firewall solution for blocking.	
2. NDR Appliance	
2.1. The proposed NDR appliance must be managed by the solutions provider, control and visibility must be extended to DBP.	
2.2. The proposed NDR appliance must include a regular (at least quarterly and/or as needed) preventive maintenance.	

ANNEX A OF FORM 9-A (page 6 of 11)

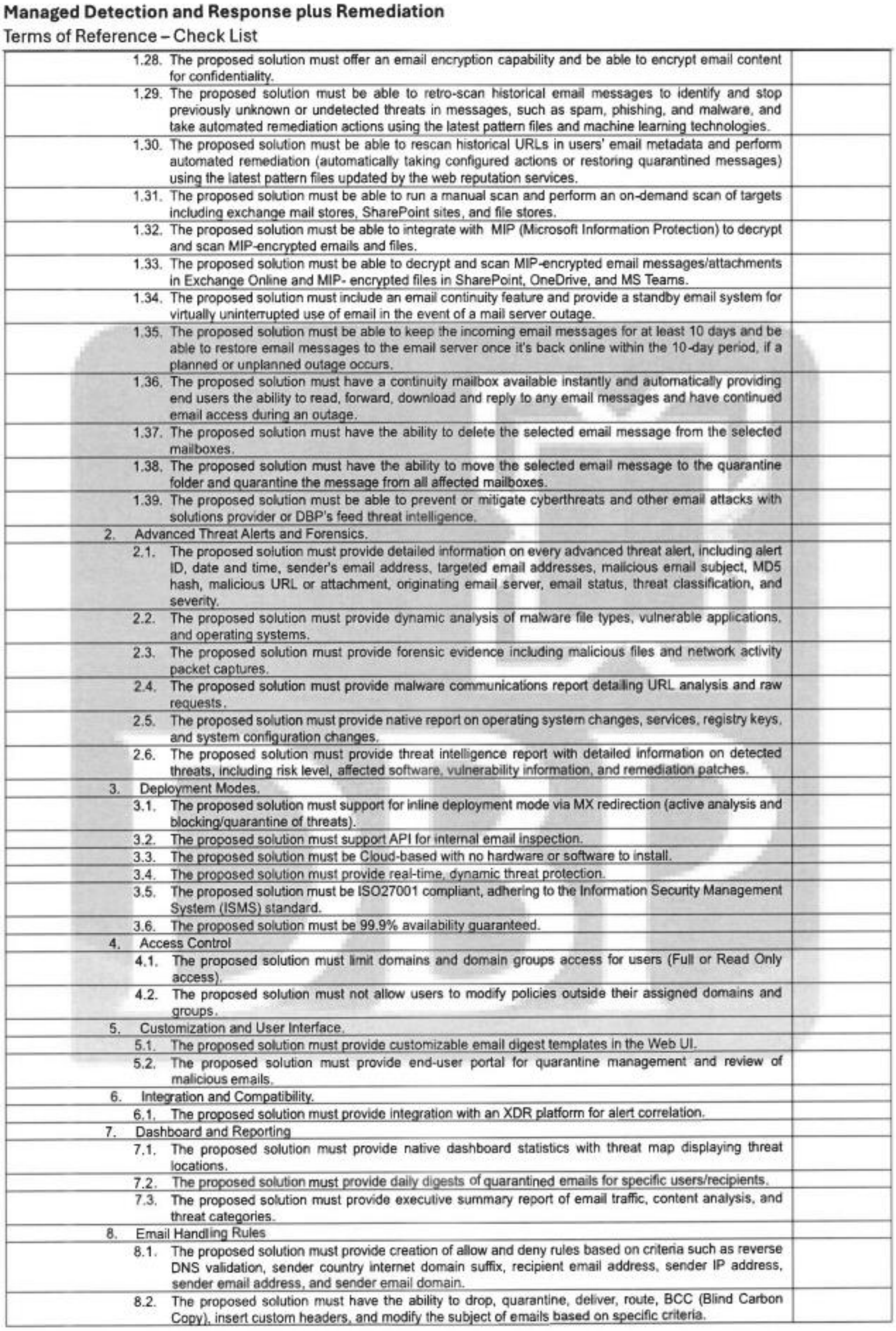


Managed Detection and Response plus Remediation

Terms of Reference – Check List

2.3. The proposed NDR appliance must include 2 units of at least 1 Gbps each.	
2.4. The proposed NDR appliance must support packet level analysis.	
2.5. The proposed NDR appliance must be installed in monitoring mode only	
2.6. The proposed NDR appliance must report to a unified XDR platform for event correlation across proposed endpoint, server and email sensors.	
3. NDR Sandboxing.	
3.1. The proposed NDR solution must support custom Windows and MacOS Sandbox.	
3.2. The proposed NDR solution must be able to provide threat execution and evaluation summary.	
3.3. The proposed NDR solution sandbox reports must be exportable.	
3.4. The proposed NDR solution must be able to track system file and registry modification.	
3.5. The proposed NDR solution must be able to detect system injection behavior detection.	
3.6. The proposed NDR solution must be able to detect network connections initiated.	
3.7. The proposed NDR solution must support the following content types for document exploits: PDF, XLS, DOC, SWF, RTF.	
3.8. The proposed NDR solution must support the following compressed files: ZIP, RAR, PKZIP, LZH.	
3.9. The proposed NDR solution must support the following Microsoft OS file formats: EXE, DLL, SYS, CHM, LNK.	
B.5. Cloud based Email Threat Security	
1. Threat Detection and Protection. 1.1. The proposed solution must have protection from AETs (Advanced Evasion Techniques) using malformed emails.	
1.2. The proposed solution must have retroactive alerting for URLs later determined to be malicious.	
1.3. The proposed solution must extract and block suspicious URLs embedded in PDF files within emails.	
1.4. The proposed solution must detect and block advanced threats in emails: attachment, URL, and impersonation-based attacks.	
1.5. The proposed solution must dynamically analyze attached files, including those with password-protection and TLS (Transport Layer Security) encryption.	
1.6. The proposed solution must have a collaboration protection capability to detect malicious files found in SharePoint, OneDrive, Teams, Google Drive, Box, and Dropbox.	
1.7. The proposed solution must have an IP reputation checking capability to block emails from known sources of spam emails (RBL- Realtime Blackhole Lists).	
1.8. The proposed solution must have domain authentication capabilities (e.g. SPF, DKIM, DMARC)	
1.9. The proposed solution must protect against spam, malware, phishing, BEC (Business Email Compromise), and ransomware email attacks.	
1.10. The proposed solution must be able to identity and detect graymail based on their category (e.g. marketing and newsletter, social network notifications, forum notifications, bulk email message)	
1.11. The proposed solution must support file sanitization (or Content Disarm and Recovery) to neutralize all unfamiliar code hiding in emails that contain active content such as macros in the email attachments.	
1.12. The proposed solution must have an attachment password guessing capability which attempts to find passwords in email content to access password-protected attachments, making it possible to scan and detect any malicious payload in these files.	
1.13. The proposed solution must have a predictive machine learning scanning capability to find unknown malware before cloud sandboxing and improve delivery efficiency.	
1.14. The proposed solution must support cloud sandboxing of suspicious file attachments and suspicious URLs found in email.	
1.15. The proposed solution must provide URL rewriting and URL time of click protection capabilities.	
1.16. The proposed solution must have a web reputation technology to scan URLs in email messages and track the credibility of web domains by assigning a reputation score based on factors including website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis, such as phishing attacks that are designed to trick users into providing personal information.	
1.17. The proposed solution must support URL extractions from QR codes to stop phishing, ransomware, and BEC attacks.	
1.18. The proposed solution must support dynamic URL scanning and crawl on the web pages of untested URLs in real-time to determine whether the pages contain malicious patterns to keep users from zero-day phishing attacks.	
1.19. The proposed solution must leverage artificial intelligence (AI)-based computer vision to analyze branded website elements and recognize fake sites to protect users against credential phishing.	
1.20. The proposed solution must have an AI-based computer vision to recognize key elements of a valid cloud service log-on page or forms to help prevent users from submitting credentials to untrusted sites and help them get rid of account compromise.	
1.21. The proposed solution must detect display name spoofing and be able to analyze messages from external senders with a look-alike display name as used in the company.	
1.22. The proposed solution's BEC detection must support adding and maintaining a list of HPU (High-Profile Users) and HPD (High-Profile Domains).	
1.23. The proposed solution's BEC detection must check the email header for behavior analysis and the email content for intention analysis.	
1.24. The proposed solution's BEC detection must support Writing Style DNA technology and provide authorship analysis to detect email attacks impersonating high-profile users.	
1.25. The proposed solution must check for unusual signals or behaviors in email (e.g. the sender has not sent any email in at least the past 30 days, unfamiliar sender discussing payment related issues, etc.)	
1.26. The proposed solution must provide account takeover protection and alert if an account has been compromised to steal data, deliver malware, or conduct internal and supply chain phishing.	
1.27. The proposed solution must offer DLP (Data Loss Prevention) capability both for email messages and files in cloud collaboration services.	

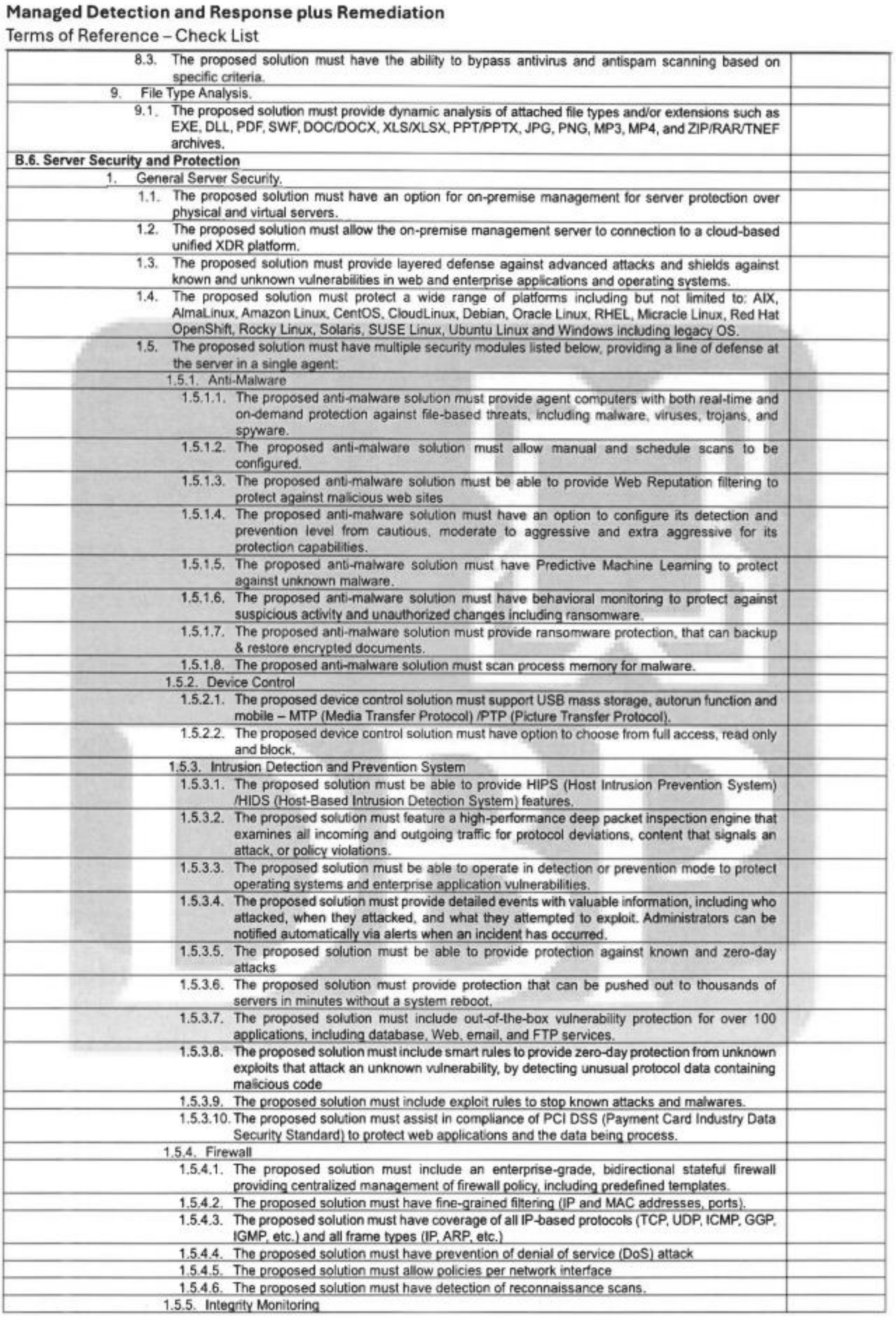
ANNEX A OF FORM 9-A (page 7 of 11)



Managed Detection and Response plus Remediation

Terms of Reference – Check List

1.28. The proposed solution must offer an email encryption capability and be able to encrypt email content for confidentiality.	
1.29. The proposed solution must be able to retro-scan historical email messages to identify and stop previously unknown or undetected threats in messages, such as spam, phishing, and malware, and take automated remediation actions using the latest pattern files and machine learning technologies.	
1.30. The proposed solution must be able to rescan historical URLs in users' email metadata and perform automated remediation (automatically taking configured actions or restoring quarantined messages) using the latest pattern files updated by the web reputation services.	
1.31. The proposed solution must be able to run a manual scan and perform an on-demand scan of targets including exchange mail stores, SharePoint sites, and file stores.	
1.32. The proposed solution must be able to integrate with MIP (Microsoft Information Protection) to decrypt and scan MIP-encrypted emails and files.	
1.33. The proposed solution must be able to decrypt and scan MIP-encrypted email messages/attachments in Exchange Online and MIP- encrypted files in SharePoint, OneDrive, and MS Teams.	
1.34. The proposed solution must include an email continuity feature and provide a standby email system for virtually uninterrupted use of email in the event of a mail server outage.	
1.35. The proposed solution must be able to keep the incoming email messages for at least 10 days and be able to restore email messages to the email server once it's back online within the 10-day period, if a planned or unplanned outage occurs.	
1.36. The proposed solution must have a continuity mailbox available instantly and automatically providing end users the ability to read, forward, download and reply to any email messages and have continued email access during an outage.	
1.37. The proposed solution must have the ability to delete the selected email message from the selected mailboxes.	
1.38. The proposed solution must have the ability to move the selected email message to the quarantine folder and quarantine the message from all affected mailboxes.	
1.39. The proposed solution must be able to prevent or mitigate cyberthreats and other email attacks with solutions provider or DBP's feed threat intelligence.	
2. Advanced Threat Alerts and Forensics.	
2.1. The proposed solution must provide detailed information on every advanced threat alert, including alert ID, date and time, sender's email address, targeted email addresses, malicious email subject, MD5 hash, malicious URL or attachment, originating email server, email status, threat classification, and severity.	
2.2. The proposed solution must provide dynamic analysis of malware file types, vulnerable applications, and operating systems.	
2.3. The proposed solution must provide forensic evidence including malicious files and network activity packet captures.	
2.4. The proposed solution must provide malware communications report detailing URL analysis and raw requests.	
2.5. The proposed solution must provide native report on operating system changes, services, registry keys, and system configuration changes.	
2.6. The proposed solution must provide threat intelligence report with detailed information on detected threats, including risk level, affected software, vulnerability information, and remediation patches.	
3. Deployment Modes.	
3.1. The proposed solution must support for inline deployment mode via MX redirection (active analysis and blocking/quarantine of threats).	
3.2. The proposed solution must support API for internal email inspection.	
3.3. The proposed solution must be Cloud-based with no hardware or software to install.	
3.4. The proposed solution must provide real-time, dynamic threat protection.	
3.5. The proposed solution must be ISO27001 compliant, adhering to the Information Security Management System (ISMS) standard.	
3.6. The proposed solution must be 99.9% availability guaranteed.	
4. Access Control	
4.1. The proposed solution must limit domains and domain groups access for users (Full or Read Only access).	
4.2. The proposed solution must not allow users to modify policies outside their assigned domains and groups.	
5. Customization and User Interface.	
5.1. The proposed solution must provide customizable email digest templates in the Web UI.	
5.2. The proposed solution must provide end-user portal for quarantine management and review of malicious emails.	
6. Integration and Compatibility.	
6.1. The proposed solution must provide integration with an XDR platform for alert correlation.	
7. Dashboard and Reporting	
7.1. The proposed solution must provide native dashboard statistics with threat map displaying threat locations.	
7.2. The proposed solution must provide daily digests of quarantined emails for specific users/recipients.	
7.3. The proposed solution must provide executive summary report of email traffic, content analysis, and threat categories.	
8. Email Handling Rules	
8.1. The proposed solution must provide creation of allow and deny rules based on criteria such as reverse DNS validation, sender country internet domain suffix, recipient email address, sender IP address, sender email address, and sender email domain.	
8.2. The proposed solution must have the ability to drop, quarantine, deliver, route, BCC (Blind Carbon Copy), insert custom headers, and modify the subject of emails based on specific criteria.	

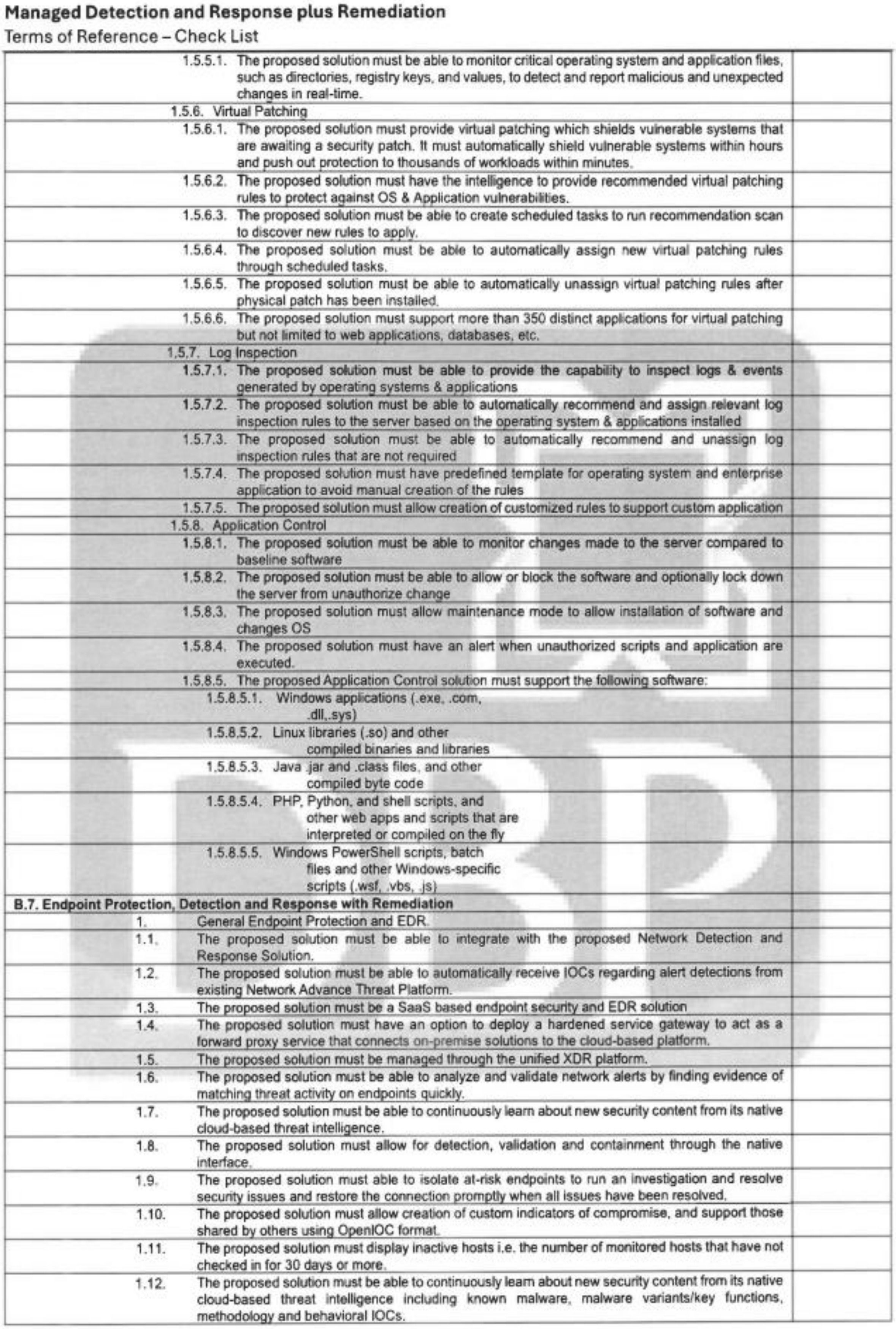


Managed Detection and Response plus Remediation

Terms of Reference – Check List

8.3. The proposed solution must have the ability to bypass antivirus and antispam scanning based on specific criteria.	
9. File Type Analysis.	
9.1. The proposed solution must provide dynamic analysis of attached file types and/or extensions such as EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4, and ZIP/RAR/TNEF archives.	
B.6. Server Security and Protection	
1. General Server Security.	
1.1. The proposed solution must have an option for on-premise management for server protection over physical and virtual servers.	
1.2. The proposed solution must allow the on-premise management server to connection to a cloud-based unified XDR platform.	
1.3. The proposed solution must provide layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.	
1.4. The proposed solution must protect a wide range of platforms including but not limited to: AIX, AlmaLinux, Amazon Linux, CentOS, CloudLinux, Debian, Oracle Linux, RHEL, Micracle Linux, Red Hat OpenShift, Rocky Linux, Solaris, SUSE Linux, Ubuntu Linux and Windows including legacy OS.	
1.5. The proposed solution must have multiple security modules listed below, providing a line of defense at the server in a single agent:	
1.5.1. Anti-Malware	
1.5.1.1. The proposed anti-malware solution must provide agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, trojans, and spyware.	
1.5.1.2. The proposed anti-malware solution must allow manual and schedule scans to be configured.	
1.5.1.3. The proposed anti-malware solution must be able to provide Web Reputation filtering to protect against malicious web sites	
1.5.1.4. The proposed anti-malware solution must have an option to configure its detection and prevention level from cautious, moderate to aggressive and extra aggressive for its protection capabilities.	
1.5.1.5. The proposed anti-malware solution must have Predictive Machine Learning to protect against unknown malware.	
1.5.1.6. The proposed anti-malware solution must have behavioral monitoring to protect against suspicious activity and unauthorized changes including ransomware.	
1.5.1.7. The proposed anti-malware solution must provide ransomware protection, that can backup & restore encrypted documents.	
1.5.1.8. The proposed anti-malware solution must scan process memory for malware.	
1.5.2. Device Control	
1.5.2.1. The proposed device control solution must support USB mass storage, autorun function and mobile – MTP (Media Transfer Protocol) /PTP (Picture Transfer Protocol).	
1.5.2.2. The proposed device control solution must have option to choose from full access, read only and block.	
1.5.3. Intrusion Detection and Prevention System	
1.5.3.1. The proposed solution must be able to provide HIPS (Host Intrusion Prevention System) /HIDS (Host-Based Intrusion Detection System) features.	
1.5.3.2. The proposed solution must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.	
1.5.3.3. The proposed solution must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.	
1.5.3.4. The proposed solution must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred.	
1.5.3.5. The proposed solution must be able to provide protection against known and zero-day attacks	
1.5.3.6. The proposed solution must provide protection that can be pushed out to thousands of servers in minutes without a system reboot.	
1.5.3.7. The proposed solution must include out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services.	
1.5.3.8. The proposed solution must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code	
1.5.3.9. The proposed solution must include exploit rules to stop known attacks and malwares.	
1.5.3.10. The proposed solution must assist in compliance of PCI DSS (Payment Card Industry Data Security Standard) to protect web applications and the data being process.	
1.5.4. Firewall	
1.5.4.1. The proposed solution must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.	
1.5.4.2. The proposed solution must have fine-grained filtering (IP and MAC addresses, ports).	
1.5.4.3. The proposed solution must have coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)	
1.5.4.4. The proposed solution must have prevention of denial of service (DoS) attack	
1.5.4.5. The proposed solution must allow policies per network interface	
1.5.4.6. The proposed solution must have detection of reconnaissance scans.	
1.5.5. Integrity Monitoring	

ANNEX A OF FORM 9-A (page 9 of 11)

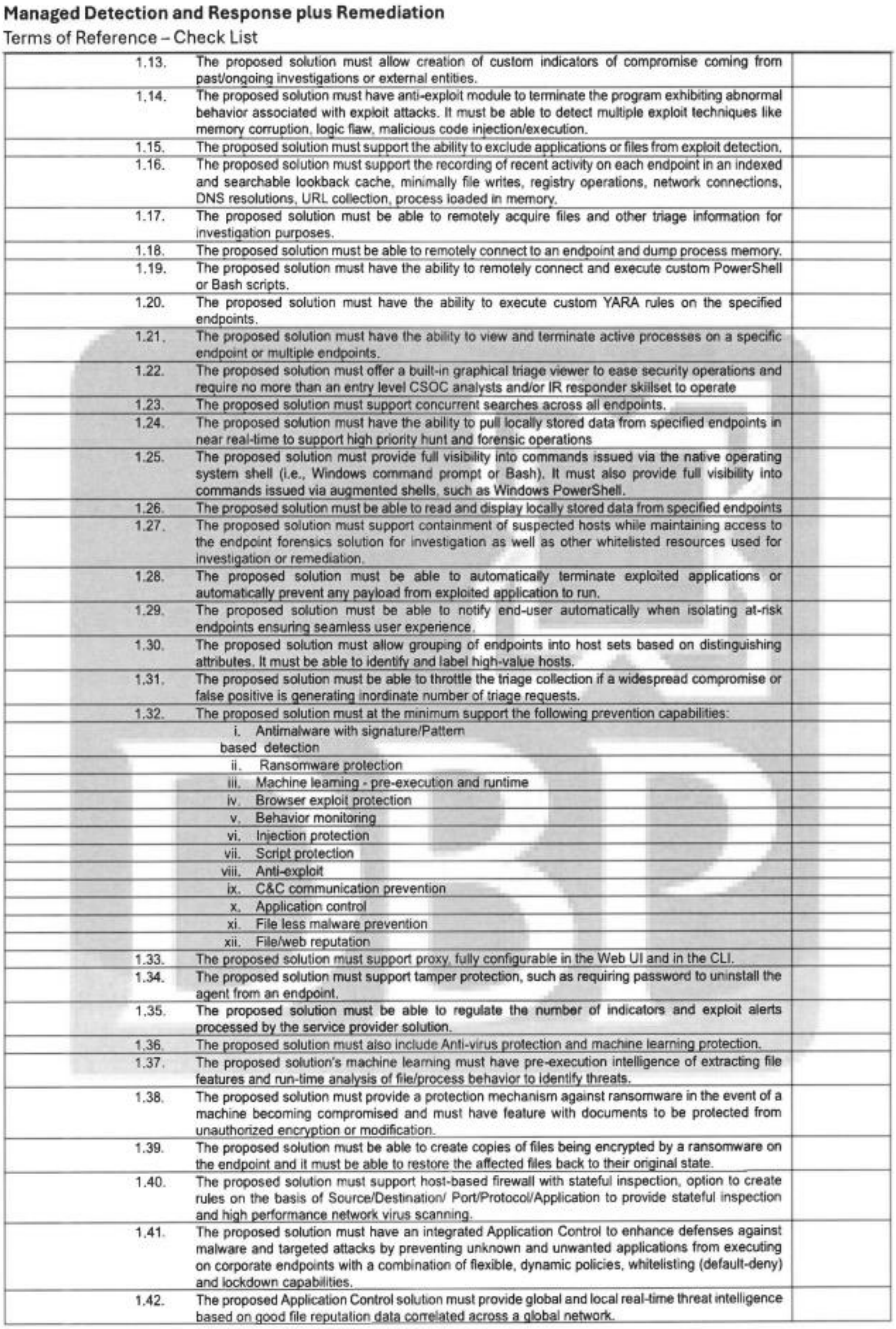


Managed Detection and Response plus Remediation

Terms of Reference – Check List

1.5.5.1. The proposed solution must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real-time.	
1.5.6. Virtual Patching	
1.5.6.1. The proposed solution must provide virtual patching which shields vulnerable systems that are awaiting a security patch. It must automatically shield vulnerable systems within hours and push out protection to thousands of workloads within minutes.	
1.5.6.2. The proposed solution must have the intelligence to provide recommended virtual patching rules to protect against OS & Application vulnerabilities.	
1.5.6.3. The proposed solution must be able to create scheduled tasks to run recommendation scan to discover new rules to apply.	
1.5.6.4. The proposed solution must be able to automatically assign new virtual patching rules through scheduled tasks.	
1.5.6.5. The proposed solution must be able to automatically unassign virtual patching rules after physical patch has been installed.	
1.5.6.6. The proposed solution must support more than 350 distinct applications for virtual patching but not limited to web applications, databases, etc.	
1.5.7. Log Inspection	
1.5.7.1. The proposed solution must be able to provide the capability to inspect logs & events generated by operating systems & applications	
1.5.7.2. The proposed solution must be able to automatically recommend and assign relevant log inspection rules to the server based on the operating system & applications installed	
1.5.7.3. The proposed solution must be able to automatically recommend and unassign log inspection rules that are not required	
1.5.7.4. The proposed solution must have predefined template for operating system and enterprise application to avoid manual creation of the rules	
1.5.7.5. The proposed solution must allow creation of customized rules to support custom application	
1.5.8. Application Control	
1.5.8.1. The proposed solution must be able to monitor changes made to the server compared to baseline software	
1.5.8.2. The proposed solution must be able to allow or block the software and optionally lock down the server from unauthorize change	
1.5.8.3. The proposed solution must allow maintenance mode to allow installation of software and changes OS	
1.5.8.4. The proposed solution must have an alert when unauthorized scripts and application are executed.	
1.5.8.5. The proposed Application Control solution must support the following software:	
1.5.8.5.1. Windows applications (.exe, .com, .dll,.sys)	
1.5.8.5.2. Linux libraries (.so) and other compiled binaries and libraries	
1.5.8.5.3. Java .jar and .class files, and other compiled byte code	
1.5.8.5.4. PHP, Python, and shell scripts, and other web apps and scripts that are interpreted or compiled on the fly	
1.5.8.5.5. Windows PowerShell scripts, batch files and other Windows-specific scripts (.wsf, .vbs, .js)	
B.7. Endpoint Protection, Detection and Response with Remediation	
1. General Endpoint Protection and EDR.	
1.1. The proposed solution must be able to integrate with the proposed Network Detection and Response Solution.	
1.2. The proposed solution must be able to automatically receive IOCs regarding alert detections from existing Network Advance Threat Platform.	
1.3. The proposed solution must be a SaaS based endpoint security and EDR solution	
1.4. The proposed solution must have an option to deploy a hardened service gateway to act as a forward proxy service that connects on-premise solutions to the cloud-based platform.	
1.5. The proposed solution must be managed through the unified XDR platform.	
1.6. The proposed solution must be able to analyze and validate network alerts by finding evidence of matching threat activity on endpoints quickly.	
1.7. The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence.	
1.8. The proposed solution must allow for detection, validation and containment through the native interface.	
1.9. The proposed solution must able to isolate at-risk endpoints to run an investigation and resolve security issues and restore the connection promptly when all issues have been resolved.	
1.10. The proposed solution must allow creation of custom indicators of compromise, and support those shared by others using OpenIOC format.	
1.11. The proposed solution must display inactive hosts i.e. the number of monitored hosts that have not checked in for 30 days or more.	
1.12. The proposed solution must be able to continuously learn about new security content from its native cloud-based threat intelligence including known malware, malware variants/key functions, methodology and behavioral IOCs.	

ANNEX A OF FORM 9-A (page 10 of 11)

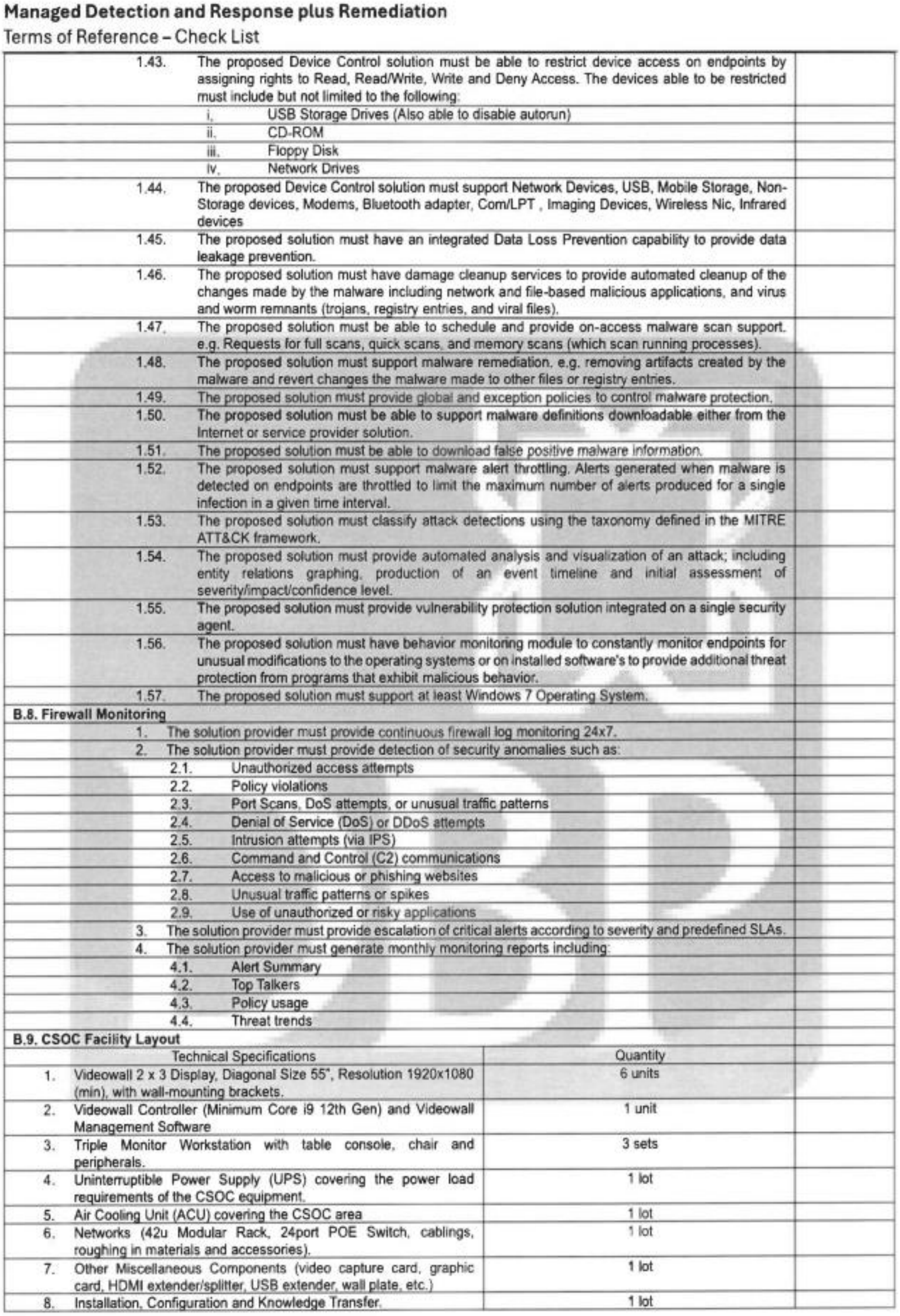


Managed Detection and Response plus Remediation

Terms of Reference – Check List

1.13.	The proposed solution must allow creation of custom indicators of compromise coming from past/ongoing investigations or external entities.	
1.14.	The proposed solution must have anti-exploit module to terminate the program exhibiting abnormal behavior associated with exploit attacks. It must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution.	
1.15.	The proposed solution must support the ability to exclude applications or files from exploit detection.	
1.16.	The proposed solution must support the recording of recent activity on each endpoint in an indexed and searchable lookback cache, minimally file writes, registry operations, network connections, DNS resolutions, URL collection, process loaded in memory.	
1.17.	The proposed solution must be able to remotely acquire files and other triage information for investigation purposes.	
1.18.	The proposed solution must be able to remotely connect to an endpoint and dump process memory.	
1.19.	The proposed solution must have the ability to remotely connect and execute custom PowerShell or Bash scripts.	
1.20.	The proposed solution must have the ability to execute custom YARA rules on the specified endpoints.	
1.21.	The proposed solution must have the ability to view and terminate active processes on a specific endpoint or multiple endpoints.	
1.22.	The proposed solution must offer a built-in graphical triage viewer to ease security operations and require no more than an entry level CSOC analysts and/or IR responder skillset to operate	
1.23.	The proposed solution must support concurrent searches across all endpoints.	
1.24.	The proposed solution must have the ability to pull locally stored data from specified endpoints in near real-time to support high priority hunt and forensic operations	
1.25.	The proposed solution must provide full visibility into commands issued via the native operating system shell (i.e., Windows command prompt or Bash). It must also provide full visibility into commands issued via augmented shells, such as Windows PowerShell.	
1.26.	The proposed solution must be able to read and display locally stored data from specified endpoints	
1.27.	The proposed solution must support containment of suspected hosts while maintaining access to the endpoint forensics solution for investigation as well as other whitelisted resources used for investigation or remediation.	
1.28.	The proposed solution must be able to automatically terminate exploited applications or automatically prevent any payload from exploited application to run.	
1.29.	The proposed solution must be able to notify end-user automatically when isolating at-risk endpoints ensuring seamless user experience.	
1.30.	The proposed solution must allow grouping of endpoints into host sets based on distinguishing attributes. It must be able to identify and label high-value hosts.	
1.31.	The proposed solution must be able to throttle the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests.	
1.32.	The proposed solution must at the minimum support the following prevention capabilities:	
	i. Antimalware with signature/Pattern based detection	
	ii. Ransomware protection	
	iii. Machine learning - pre-execution and runtime	
	iv. Browser exploit protection	
	v. Behavior monitoring	
	vi. Injection protection	
	vii. Script protection	
	viii. Anti-exploit	
	ix. C&C communication prevention	
	x. Application control	
	xi. File less malware prevention	
	xii. File/web reputation	
1.33.	The proposed solution must support proxy, fully configurable in the Web UI and in the CLI.	
1.34.	The proposed solution must support tamper protection, such as requiring password to uninstall the agent from an endpoint.	
1.35.	The proposed solution must be able to regulate the number of indicators and exploit alerts processed by the service provider solution.	
1.36.	The proposed solution must also include Anti-virus protection and machine learning protection.	
1.37.	The proposed solution's machine learning must have pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.	
1.38.	The proposed solution must provide a protection mechanism against ransomware in the event of a machine becoming compromised and must have feature with documents to be protected from unauthorized encryption or modification.	
1.39.	The proposed solution must be able to create copies of files being encrypted by a ransomware on the endpoint and it must be able to restore the affected files back to their original state.	
1.40.	The proposed solution must support host-based firewall with stateful inspection, option to create rules on the basis of Source/Destination/ Port/Protocol/Application to provide stateful inspection and high performance network virus scanning.	
1.41.	The proposed solution must have an integrated Application Control to enhance defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting (default-deny) and lockdown capabilities.	
1.42.	The proposed Application Control solution must provide global and local real-time threat intelligence based on good file reputation data correlated across a global network.	

ANNEX A OF FORM 9-A (page 11 of 11)



Managed Detection and Response plus Remediation

Terms of Reference – Check List

1.43.	The proposed Device Control solution must be able to restrict device access on endpoints by assigning rights to Read, Read/Write, Write and Deny Access. The devices able to be restricted must include but not limited to the following:		
i.	USB Storage Drives (Also able to disable autorun)		
ii.	CD-ROM		
iii.	Floppy Disk		
iv.	Network Drives		
1.44.	The proposed Device Control solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Modems, Bluetooth adapter, Com/LPT , Imaging Devices, Wireless Nic, Infrared devices		
1.45.	The proposed solution must have an integrated Data Loss Prevention capability to provide data leakage prevention.		
1.46.	The proposed solution must have damage cleanup services to provide automated cleanup of the changes made by the malware including network and file-based malicious applications, and virus and worm remnants (trojans, registry entries, and viral files).		
1.47.	The proposed solution must be able to schedule and provide on-access malware scan support. e.g. Requests for full scans, quick scans, and memory scans (which scan running processes).		
1.48.	The proposed solution must support malware remediation. e.g. removing artifacts created by the malware and revert changes the malware made to other files or registry entries.		
1.49.	The proposed solution must provide global and exception policies to control malware protection.		
1.50.	The proposed solution must be able to support malware definitions downloadable either from the Internet or service provider solution.		
1.51.	The proposed solution must be able to download false positive malware information.		
1.52.	The proposed solution must support malware alert throttling. Alerts generated when malware is detected on endpoints are throttled to limit the maximum number of alerts produced for a single infection in a given time interval.		
1.53.	The proposed solution must classify attack detections using the taxonomy defined in the MITRE ATT&CK framework.		
1.54.	The proposed solution must provide automated analysis and visualization of an attack; including entity relations graphing, production of an event timeline and initial assessment of severity/impact/confidence level.		
1.55.	The proposed solution must provide vulnerability protection solution integrated on a single security agent.		
1.56.	The proposed solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems or on installed software's to provide additional threat protection from programs that exhibit malicious behavior.		
1.57.	The proposed solution must support at least Windows 7 Operating System.		
B.8. Firewall Monitoring			
1.	The solution provider must provide continuous firewall log monitoring 24x7.		
2.	The solution provider must provide detection of security anomalies such as:		
2.1.	Unauthorized access attempts		
2.2.	Policy violations		
2.3.	Port Scans, DoS attempts, or unusual traffic patterns		
2.4.	Denial of Service (DoS) or DDoS attempts		
2.5.	Intrusion attempts (via IPS)		
2.6.	Command and Control (C2) communications		
2.7.	Access to malicious or phishing websites		
2.8.	Unusual traffic patterns or spikes		
2.9.	Use of unauthorized or risky applications		
3.	The solution provider must provide escalation of critical alerts according to severity and predefined SLAs.		
4.	The solution provider must generate monthly monitoring reports including:		
4.1.	Alert Summary		
4.2.	Top Talkers		
4.3.	Policy usage		
4.4.	Threat trends		
B.9. CSOC Facility Layout			
	Technical Specifications	Quantity	
1.	Videowall 2 x 3 Display, Diagonal Size 55", Resolution 1920x1080 (min), with wall-mounting brackets.	6 units	
2.	Videowall Controller (Minimum Core i9 12th Gen) and Videowall Management Software	1 unit	
3.	Triple Monitor Workstation with table console, chair and peripherals.	3 sets	
4.	Uninterruptible Power Supply (UPS) covering the power load requirements of the CSOC equipment.	1 lot	
5.	Air Cooling Unit (ACU) covering the CSOC area	1 lot	
6.	Networks (42u Modular Rack, 24port POE Switch, cablings, roughing in materials and accessories).	1 lot	
7.	Other Miscellaneous Components (video capture card, graphic card, HDMI extender/splitter, USB extender, wall plate, etc.)	1 lot	
8.	Installation, Configuration and Knowledge Transfer.	1 lot	

FORM 10 (page 1 of 2)

(use Bidder's Official Letterhead)

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

BID FORM

Date : _________________

Bid Reference No. : _________________

To: DEVELOPMENT BANK OF THE PHILIPPINES

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.

	Approved Budget of the Contract (in PhP), inclusive of taxes		***Bid Offer (in PhP), inclusive of taxes***	
	Per Year	***For 3 Years***	***For One Year***	***For 3 Years***
Amount in Figures	55,000,000.00	165,000,000.00		
Amount in Words	Fifty-Five Million Pesos	One Hundred Sixty-Five Million Pesos		

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.

FORM 10 (page 2 of 2)

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.

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: ___________________

FORM 11-A

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

Price Schedule for Goods Offered from Within the Philippines

[shall be submitted with the Bid if bidder is offering goods from within the Philippines]

Name of Bidder ________________________ Project ID No._________ Page ___of___

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of origin	Quantity	Unit price EXWper item	Transportation and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)

The total bid must not exceed the total ABC and must be consistent with the financial bid per FORM 10.

Name: ____

Legal Capacity: ____

Signature: ____

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

FORM 11-B

ONE (1) LOT SUPPLY, DELIVERY, INSTALLATION, CONFIGURATION AND SUBSCRIPTION OF MANAGED DETECTION AND RESPONSE PLUS REMEDIATION (MDR+R) SOLUTION FOR THE DEVELOPMENT BANK OF THE PHILIPPINES
Bid Reference No. G-2025-20

Price Schedule for Goods Offered from Abroad

[shall be submitted with the Bid if bidder is offering goods from Abroad]

Name of Bidder ___________________________ Project ID No.__________ Page ___ of ___

1	2	3	4	5	6	7	8	9
Item	Description	Country of origin	Quantity	Unit price CIF port of entry (specify port) or CIPnamed place (specify border point or place of destination)	Total CIFor CIPprice per item (col. 4 x 5)	Unit Price Delivered Duty Unpaid (DDU)	Unit priceDelivered Duty Paid (DDP)	Total Price delivered DDP (col 4 x 8)

The total bid must not exceed the total ABC and must be consistent with the financial bid per FORM 10.

Name: ____

Legal Capacity: ____

Signature: ____

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

Section X. Post-Qualification Documents

POST-QUALIFICATION TRANSMITTAL FORM

TITLE OF THE PROJECT:____

Note: For the SINGLE/LOWEST CALCULATED BID (S/LCB), please fill-out and submit together with the Post Qualification Requirements

FOR MACHINE STAMP (OFFICIAL TIME) BY THE DBP BAC SECRETARIAT Received:

Name of Bidder:____

Complete Address:____

Submitted by:____

Landline:_______________________________________Email:_____________

Within five (5) calendar days from the notice that the bidder is the **Lowest or Single Calculated Bid (LCB/SCB)**, the bidder shall submit two (2) sets of the following documentary requirements (which the bidder may also opt to submit on the date of opening of proposals; please bring ORIGINAL documents for verification):

i. Latest Annual Income Tax Returns;

ii. Latest Business Tax Returns: VAT Returns (Form 2550M and 2550Q) or Percentage Tax Returns (2551M) for the six (6) months period preceding the submission and opening of bids with proof of payment (any one of the following):

   a. Electronic Filing and Payment System (EFPS) confirmation receipt
   b. Bank-issued payment confirmation receipt
   c. BIR payment confirmation receipts/status

iii. Copies of the following documents:

   a. DTI or SEC Certificate of Registration (including the names of company's controlling stockholders, directors, board members and officers);
   b. General Information Sheet (GIS) (as attached in the SEC Certificate of Registration)
   c. Valid/current Business/Mayor's Permit; and
   d. Valid/current Tax Clearance issued by the BIR for bidding purposes.

iv. Copies of Notice of Award (NOA), contract, Notice to Proceed (NTP), or equivalent documents relative to the listed ongoing projects/contracts.

v. Duly signed Letter of Authorization stating that the bidder is authorizing the Development Bank of the Philippines (DBP) to conduct credit/background investigation as part of the Post-Qualification process, in relation to the project being bid. *(Template hereto attached)*

vi. Other documents as may be listed in the Technical Specifications/Terms of Reference/Scope of Works.

Note: Failure to submit the above requirements on time or a finding against the veracity of such shall be grounds for the forfeiture of the bid security and disqualify the bidder for award.

LETTER OF AUTHORIZATION

[shall be submitted during post-qualification process or upon receipt of the Notice of Single/Lowest Calculated Bid]

(use Bidder's Official Letterhead)

Date:

To: **THE CHAIRPERSON, BIDS AND AWARDS COMMITTEE (BAC)**
Development Bank of the Philippines (DBP)
Sen. Gil Puyat Ave., cor. Makati Ave., Makati City
1200 Philippines

Gentlemen:

This is to authorize the Development Bank of the Philippines (DBP) and its authorized representatives, to conduct the validation/verification of the following documents as part of post qualification relative to our bid for the *(state Title of the Bid Project)* under *(state Bid Reference Number)*:

1. Certificate of PhilGEPS Registration (Platinum Membership)
2. SEC or DTI Certificate of Registration (as applicable)
3. Current/Valid Business/Mayor's Permit
4. Current/Valid Tax Clearance
5. Current Audited Financial Statements
6. Current/Valid PCAB License (only applicable for Infrastructure projects)
7. Completed Contract/s

Thank you.

Very truly yours,

____
Name and Signature of the Authorized Representative

Section XI. Performance Securing Declaration Form

Performance Securing Declaration

[if used as an alternative performance security but it is not required to be submitted with the Bid, as it shall be submitted within ten (10) days after receiving the Notice of Award]

____

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

PERFORMANCE SECURING DECLARATION

Invitation to Bid: [Insert Reference Number indicated in the Bidding Documents]
To: [Insert name and address of the Procuring Entity]

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, to guarantee the faithful performance by the supplier/distributor/manufacturer/contractor/consultant of its obligations under the Contract, I/we shall submit a Performance Securing Declaration within a maximum period of ten (10) calendar days from the receipt of the Notice of Award prior to the signing of the Contract.

2. I/We accept that: I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of one (1) year for the first offense, or two (2) years **for the second offense**, upon receipt of your Blacklisting Order if I/We have violated my/our obligations under the Contract;

3. I/We understand that this Performance Securing Declaration shall cease to be valid upon:

   a. issuance by the Procuring Entity of the Certificate of Final Acceptance, subject to the following conditions:
      i. Procuring Entity has no claims filed against the contract awardee;
      ii. It has no claims for labor and materials filed against the contractor; and
      iii. Other terms of the contract; or

   b. replacement by the winning bidder of the submitted PSD with a performance security in any of the prescribed forms under Section 39.2 of the 2016 revised IRR of RA No. 9184 as required by the end-user.

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

SUBSCRIBED AND SWORN to before me this __ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her *[insert type of government identification card used]*, with his/her photograph and signature appearing thereon.

Witness my hand and seal this ___ day of *[month] [year].*

NAME OF NOTARY PUBLIC
Serial No. of Commission _______________
Notary Public for __________ until ________
Roll of Attorneys No.____________________
PTR No._____, *[date issued], [place issued]*
IBP No.______, *[date issued], [place issued]*

Doc. No. __________
Page No. __________
Book No. __________
Series of __________

Section XII. Draft Contract/ Purchase Order

Contract Agreement Form for the Procurement of Goods (Revised)

[Not required to be submitted with the Bid, but it shall be submitted within ten (10) days after receiving the Notice of Award]

DRAFT 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;

      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;

   iii. 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**

<u>submission after the contract execution, such as the Notice to Proceed, Variation Orders, and Warranty Security, shall likewise form part of the Contract.</u>

3. In consideration for the sum of *[totalcontract 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 Signatory's Legal Capacity]

for:

[Insert Procuring Entity]

[Insert Name and Signature]

[Insert Signatory's Legal Capacity]

for:

[Insert Name of Supplier]

<u>Acknowledgment</u>

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

DBP Development Bank of the Philippines

PURCHASE ORDER

SUPPLIER :	P.O. NO. :
	DATE :
ADDRESS :	END USER :
	P.R. NO. :
TIN :	
TEL./FAX NO. :	MODE OF PROCUREMENT :

Gentlemen:

Please deliver the following article(s), product(s), supplies, or materials listed below, subject to the terms and conditions contained herein:

DESCRIPTION/BRAND/STOCK NO./PRODUCT CODE	QTY.	UNIT	UNIT PRICE	AMOUNT
			TOTAL AMOUNT:	

TOTAL AMOUNT IN WORDS :	
PLACE OF DELIVERY :	DELIVERY TERM :
DATE OF DELIVERY :	PAYMENT TERM :
TIME OF DELIVERY :	COUNTRY OF ORIGIN :

Subject to the following conditions:

1. The above prices are inclusive of V.A.T.
2. For every day of delay, 1/10 of 1% of the price of the undelivered quantity will be deducted from the total price.
3. Items delivered are subject to inspection and acceptance prior to payment.
4. When requesting payment, please present your Billing Statement/Statement of Account/Sales Invoice/Charge Slip, as the case may be.
5. If delivery cannot be completed within the specified date, please return this P.O. stating your reason(s) therefore. Otherwise, we will take necessary action to protect the interest of the DBP.
6. This transaction shall be subjected to the specific terms and conditions set forth in the Terms of Reference/Scope of Works/Technical Specifications.
7. Further, the following documents shall be attached, deemed to form, and be read and construed as part of this Purchase Order, to wit:
   - General and Special Conditions of Contract;
   - Terms of Reference/Scope of Works/Technical Specifications; and
   - Other contract documents that may be required by existing laws and/or DBP
8. For the avoidance of doubt, in the conflict or inconsistency between the above-mentioned documents and this Purchase Order of precedence shall be:
   - The General and Special Conditions of Contract;
   - The Terms of Reference/Scope of Work/Technical Specifications; and
   - This Purchase Order

PROCESSED :	We accept this Purchase Order with all its terms and conditions. We certify that we have not given nor di we intend to give any amount of money or gift in any form whatsoever to any official or employee of the DBP for the purpose of securing this P.O. or having the payment hereof expedited. We understand and accept that such acts on our part shall constitute sufficient ground for the DBO to revoke this P.O. and cause us to be excluded from further dealings with the Bank.
CHECKED :	(Printed Name of Supplier / Contractor) By: (Duly Authorized Representative)
	SIGNATURE :
APPROVED :	NAME :
	POSITION :
	DATE :

HEAD OFFICE: SEN. GIL J. PUYAT AVENUE CORNER MAKATI AVENUE, MAKATI CITY, PHILIPPINES
P.O. BOX 1996, MAKATI CENTRAL POST OFFICE 1200
TELEPHONE: (02) 8818-95-11
FAX NO.: (02)8815-16-14
E-MAIL: pimd@dbp.ph

Republic of the Philippines

gppb

Government Procurement Policy Board