



MORMUGAO PORT TRUST
INFORMATION TECHNOLOGY CELL
FINANCE DEPARTMENT

FA/IT(7-AV)/2018/369

07.08.2018

To

1. M/s ADD-ON Systems IT Services Pvt. Ltd.
2. M/s Accel Frontline Pvt. Ltd.
3. M/s Magnamious System Pvt. Ltd.
4. M/s PC Station
5. M/s Silicon Computers Pvt. Ltd.
6. M/s Winsys Systems Pvt. Ltd.

Dear Sir,

Last Date and Time for Submission of Tender: 23.08.2018 on or before 15.00 hrs.

Sub : Supply & Installation of Anti-Virus and Endpoint Protection Solution.

Ref : Tender No. FA/IT(7-AV)/2018/369 due on 23.08.2018 at 15.00 hrs.

EMD: Rs.11400.00 (Rupees Eleven Thousand Four Hundred only)

Mormugao Port Trust (MPT) is inviting bids for supply/installation of Anti-Virus and Endpoint Protection Solution for 350 seats for a period of three years and On-Site Support Services in sealed double cover system at the following address:

Asst. Director (EDP),
IT Cell, Finance Department,
1st Floor, Administrative Building,
Headland Sada, Goa 403 804.
Phone No. 0832-2594419, 2594423

The sealed tender (double cover system comprising of Technical Bid Cover and Price Bid Cover) should reach the Assistant Director (EDP) up to 15:00 hours on 23.08.2017. The Technical Bid will be opened on the same day at 15:30 hours in the Conference Room located on the first floor of the Finance Department at Administrative Building, Headland Sada, Goa in the presence of representatives of tenderers who wish to be present. Bids received after due date and time are liable to be rejected. The sealed envelope should be superscribed as "Bid for Anti-Virus and Endpoint Protection Solution" containing therein sealed Technical Bid cover and sealed Price Bid Cover. Those Bids which meet minimum eligibility criteria and fulfilling other requirements will be considered for further evaluation.

The Technical Bid shall contain complete & detailed technical specifications as per Technical Specifications specified in Annexure A, Technical Bid Compliance Checklist

as per Annexure B, acceptance of Commercial Terms and Conditions and Demand Draft/Payment Details towards EMD. The Price Bid should include only price. Both the covers to be sealed and to be enclosed in another sealed envelope.

Tenders shall be accompanied by EMD of **Rs.11400.00 (Rupees Eleven Thousand Four Hundred only)**. **The EMD shall be paid in Cash/DD/NEFT/IBT in our bank before submission of bids. Our Bank details are enclosed as Annexure C.** For exemption of EMD, the certificate from SSI/MSME/NSIC or any empowered central/state Govt. authority shall be submitted. Incomplete tenders or tenders without EMD will not be accepted. Tenders should be kept valid for a minimum period of **90** days from the date of opening and shall conform to the Terms and Conditions of the Tender.

The administration reserves the right to reject any or all tenders or accept any tender wholly or in part without assigning any reason whatsoever.

Yours faithfully,

sd/-

Financial Adviser & Chief Accounts Officer

MORMUGAO PORT TRUST
INFORMATION TECHNOLOGY CELL
FINANCE DEPARTMENT

Instructions to Tenderers

1. **Tenders received before the last date and time will be opened on due date at 15.30 hrs.** The bidders or their representatives can witness the tender opening if desired.
2. The tenderers shall deposit the **Earnest Money Deposit** amount of **Rs.11400.00 (Rupees Eleven Thousand Four Hundred only)** by Cash/DD/NEFT/IBT in our Bank as per the bank details attached. For exemption of EMD, the certificate from SSI/MSME/NSIC or any empowered central/state Govt. authority shall be submitted. The details towards the EMD payment made shall be indicated in the cover. **Offers without the Earnest Money Deposit will not be considered.**
3. The Earnest Money Deposits of unsuccessful tenderers will be refunded by NEFT/IBT after a decision has been reached as regards to the acceptance of the tender. Kindly furnish your full bank details along with your offer.
4. The prices should be quoted item wise separately. Prices quoted on lump sum basis (i.e. one amount for all the items taken together) will not be considered and the offer is liable to be rejected.
5. Offers should not contain any sort of conditional discounts based on quantity or value of order. Offers containing such conditional discounts will be rejected.
6. The Tenderer has to quote separately for Sr. No.1 i.e. Supply and Installation of Anti-Virus and Endpoint Protection Software with license subscription for three years and Sr.No.2 i.e. Three Year On-Site Support (including re-installations & extra visits if required) as well as weekly visit of engineer to MPT Site for three years.
7. GST will be paid extra as applicable. Any statutory changes in taxes can be considered only if these changes occur within the contractual delivery period.
8. The Tender Documents should be signed and submitted in acceptance of all the Terms and Conditions mentioned therein. In case this is not done the tender is liable to be rejected.
9. The offer submitted should be for supply of Anti-Virus & Endpoint Protection Software for 350 seats for three years licensed subscription and three years On-Site Support Services as specified in the attached Annexure-'A', else the offer is liable to be rejected.
10. If the offers are found to deviate from our Commercial Terms & Conditions and Technical Specifications they are liable to be rejected.
11. The Administration reserves the right to reject any tender in part or in whole without assigning any reason for doing so.

FINANCIAL ADVISER & CHIEF ACCOUNTS OFFICER

NOTE: The above format should be attached to your offer duly signed and stamped failing which your offer will be considered as incomplete and liable for rejection. Further, ensure that every page is signed and stamped.

MORMUGAO PORT TRUST
INFORMATION TECHNOLOGY CELL
FINANCE DEPARTMENT

COMMERCIAL TERMS AND CONDITIONS

1. **PRICES:** Prices quoted should be as per the Price Bid format. GST will be paid extra as applicable. The prices should be firm for a period of 90 days from the date of opening of the tender. However, in case of any statutory revision in taxes within the validity period of tender, the same will be considered provided you furnish documentary evidence such as copy of Govt. notification. The Prices should include First Level Support Charges for installation & commissioning of the Software.
2. **QUANTITY:** 350 seats with license subscription for three years.
3. **DELIVER:** The Software should be installed and activated within ten days from the date of Work Order.
4. **PAYMENT:** Payment towards supply and installation of software shall be made by NEFT/IBT within 15 days of successful Installation of Anti-Virus & Endpoint Protection Software. Payment towards weekly visit for three years On-Site Support for performing/monitoring of Anti-Virus/Spyware activities shall be paid on quarterly basis after completion of the quarter.
5. **EMD :** The tenderers shall furnish the **Earnest Money Deposit (EMD)** amount of **Rs.11400.00 (Rupees Eleven Thousand Four Hundred only)** by Cash or DD drawn in favour of "Financial Adviser and Chief Accounts Officer, Mormugao Port Trust" along with the tender or remit by NEFT/IBT to our Account as per the bank details attached. For exemption of EMD, the certificate from SSI/MSME/NSIC or any empowered central/state Govt. authority shall be submitted. The details towards the EMD payment made shall be indicated in the cover. **Offers without the Earnest Money Deposit will not be considered.** Failure to comply with the Tender Conditions will entail forfeiture of EMD amount.
6. **SECURITY DEPOSIT:** Within 14 days of acceptance of the tender, the successful tenderer will have to affect a Security Deposit equal to 10% of the total value of the Rate Contract by Demand Draft or by Bank Guarantee from a Scheduled Bank. The Demand Draft should be drawn in favour of the Financial Advisor and Chief Accounts Officer, Mormugao Port Trust, Goa payable at Mormugao Harbour, Goa. However, in case the Security Deposit is furnished by way of Bank Guarantee, the same should be valid for a minimum period of 36 months from the date of installation of software with a claim period of further 2 months.
7. **LIQUIDATED DAMAGES:** Supply schedule as per order should be strictly adhered to. In the event of delay in supplies, Liquidated Damages at 0.5% of the total basic value quoted at Sr.No. 1 of the Price Bid will be levied per week or part thereof of delay. The total Liquidated Damages shall however not exceed 5% of the total basic value quoted at Sr.No.1 of the Price Bid. The total value here means the total value of Supply/Installation of Anti-virus & Endpoint Protection Software Licenses exclusive of taxes etc. **The date of installation of Anti-Virus Software and activation of licenses at our site at Headland Sada, Goa will be considered as date of delivery for the purpose of Liquidated Damages.**

8. **FORCE MAJEURE & EXTENSION IN DELIVERY PERIOD:** In case of failure to supply, install Anti-Virus Software and activate the licenses in time which shall have arisen due to war, insurrection, restraint imposed by the Government Act or Legislation or other Authority, accident, strike, riot, lock-out or unforeseen events beyond human control directly or indirectly interfering with the supply/installation of Software and activation of licenses or from any cause which the purchaser may admit as reasonable ground for an extension of time, the purchaser will allow such additional time he considers reasonable provided that the contractor shall report to the purchaser the occurrence of any cause as aforesaid which will or might affect the performance of the contract within a reasonable time. Requests for extension received after expiry of the delivery schedule will not be entertained.
9. **ON-SITE SUPPORT SERVICES:** Three Year On-Site Support Services include Weekly Visit of Service Engineer to MPT Site. The Tenderer has to depute Service Engineer every week to MPT site during the validity of contract. Proportionate amount would be deducted if the visits are less than the scheduled. If the support activities during each weekly visit remained incomplete and spills over the next day or so on, the work has to be completed. Consequently, the visit would be treated as if only one day without any additional cost. The Tenderer has to ensure that the Support Engineer submits report about the observations and activities carried out during the weekly visit. The Service Engineer is required to carry out the following tasks.
- i) Reinstallation of Anti-Virus and Endpoint Protection Software if required during the year.
 - ii) Monitoring of Anti-virus Servers and Solution for entire landscape in case some clients are not getting automatically updated from server, updating them and later configuring them for auto-update.
 - iii) Cleaning the infected systems with latest patches/antivirus pattern file and removing the viruses without formatting the system as far as possible.
 - iv) Ensure that the antivirus solution is up to date and should be able to detect latest viruses and trojan.
 - v) Spyware Detection & Network Threat Protection.
 - vi) O.S. Patch Updates.
 - vii) Ensuring Redundant Anti-Virus and Endpoint Protection Server functions with all the parameters in the event of failure of Primary Anti-Virus and Endpoint Protection Server.
 - viii) Enabling/Disabling external USB devices.
 - ix) Any other tasks pertaining to Anti-Virus and Endpoint Protection Software functionality.
10. **ADDITIONAL DETAILS :** The full details as regards Permanent Account Number (PAN) (Income Tax) Bank A/C No. and type of A/C, Name, Address, MICR Code and IFSC Code of Bank, GST etc. should be furnished as per the formats specified in attached Annexures.
11. **JURISDICTION:** In case of any dispute the jurisdiction will be GOA only.

We hereby agree to all the above terms and conditions.

Signature and Seal of Tenderer

NOTE: This above format should be included in Technical Bid Cover of your offer duly signed and stamped, failing which your offer will be considered as incomplete and liable for rejection.

MORMUGAO PORT TRUST
INFORMATION TECHNOLOGY CELL
FINANCE DEPARTMENT

CONDITIONS OF CONTRACT

1. DEFINITIONS:

PURCHASER means “FINANCIAL ADVISER & CHIEF ACCOUNTS OFFICER* on behalf of the Chairman of the Board of Trustees of Mormugao Port trust.

“VENDOR” means the person, firm or company whose tender is accepted.

2. **CONTRACT:** This contract is for at the rate in the quotation and within the time specified in the Purchase Order.
3. **DELIVERY:** The Vendor is bound to supply licenses in 10 days.
4. **PAYMENT:** The payment for Anti-virus and Endpoint Protection software for 350 seats with three years licensed subscription will be effected on successful implementation of the software. The payment for weekly on-site support activities would be effected on completion of every quarter.
5. The Administration reserves the right to accept/reject in part or in whole the tender without assigning any reason whatsoever.

Contractors Signature

NOTE: The above format should be included in Technical Bid offer duly signed and stamped failing which your offer will be considered as incomplete and liable for rejection. Further, ensure that every page is signed and stamped.



MORMUGAO PORT TRUST
INFORMATION TECHNOLOGY CELL
FINANCE DEPARTMENT

TENDER FORM

To
FA & CAO
Mormugao Port Trust,
1st Floor, A.O. Bldg.,
Headland, Sada, Mormugao,
Goa - 403 804.

I/we _____ do hereby tender to supply and install _____ (Name of Anti-Virus and Endpoint Protection Software) with subscription of three year at the prices quoted by us and as per Technical Specifications and other Terms and Conditions of the Tender.

I/We further agree, that if my/our tender is accepted to effect within 14 days of such acceptance a deposit with the Financial Advisor and Chief Account Officer, Mormugao Port Trust, Headland Sada, Mormugao, Goa (in cash, by Demand Draft or in the form of Bank Guarantee from any scheduled Bank) equal to 10% of the for which the tender has been accepted.

Signature of the Contractor

Name: _____

Address: _____

Witness: 1. _____

2. _____

REMARKS: Kindly submit this form duly signed and stamped in your Technical Bid or else your offer is liable to be rejected.

PRICE SCHEDULE COVER

TENDER NO. FA/IT(7-AV)/2018/329 DUE ON: 11.06.2018

Sr No	Description	Quantity (No. of Seats)	Rate exclusive of GST (Rs.)	Amount (Rs.) exclusive of GST
A	B	C	D	E=(C * D)
1	Supply/Installation of Anti-Virus and Endpoint Protection Software for one year for 350 seats licensed for three years. The Prices should include First Level Support Charges for installation & commissioning of the Software.	350		
2	Three Year On-site Support (including Re-installation & extra Visits if required) and Weekly Visit of Engineer for three years.	1		
	Total (Sr. No. 1 + Sr. No. 2)			

1. The tenderers are requested to fill up the above details in the Price Schedule and enclose in the cover.
2. Item mentioned at Sr. No. 2 is optional.
3. Evaluation of the Bid would be done on the basis of total amount of items at Sr. No. 1 and 2 specified in the above format.
4. Offers not given in above format are liable to be rejected.
5. GST - Goods & Services Tax is payable extra as applicable

Date: _____

Name, Signature & Seal of the Tenderer

MORMUGAO PORT TRUST
INFORMATION TECHNOLOGY CELL
MINIMUM ELIGIBILITY CRITERIA

1.0 FINANCIAL ELIGIBILITY:

1.1 Bidder's experience of having successfully completed the work of supply & installation of End Point Protection and Anti-Virus Suite during the last three years from the due date of submission of bid. The Work Order as well as completion date should be within last 3 years from the due date of submission of bid. Copy of the Purchase/Work Order along with corresponding completion certificate from the client should be furnished. The completed works should be either of the following:-

1.1.1 Three similar completed works of not less than Rs.2,29,000/- OR

1.1.2 Two similar completed works of not less than Rs.3,43,000/- OR

1.1.3 One similar completed works of not less than Rs.4,58,000/-

1.2 Similar Work means "Supply and Installation of End-Point Protection & Anti-Virus Software.

2.0 TECHNICAL ELIGIBILITY

2.1 The End Point Protection and Anti-Virus Suite should be in accordance with the specifications detailed in Annexure A & B. However, Optional Specifications specified at T.2 will not be considered for evaluation.

2.2 The Bidder is required to furnish Annexure B duly filled in with appropriate response as proof of compliance of Technical Specifications.

MORMUGAO PORT TRUST

TECHNICAL SPECIFICATIONS OF ANTI-VIRUS & ENDPOINT PROTECTION SOLUTION

T.1 : Base System

1. The Anti-Virus Solution should be able to detect and block malicious software in real time, including viruses, worms, Trojans, spyware, Adware and Root Kits, Bots etc.
2. The Anti-virus Solution must automatically scan all external storage devices, immediately when connected to the network.
3. The Anti-Virus Solution should include a behavioural based technology apart from providing the signatures for vulnerability and heuristic based approach. It should be able to score both good and bad behaviours of unknown applications, enhancing detection and reducing false positives without the need to create rule- based configurations to provide protection from unseen threats i.e. zero-day threats.
4. The Anti-virus Solution should provide enhanced anti-virus protection for desktops, laptops & servers from all the attacks originating from places inside/outside network due to virus and/or other malicious programming code and should provide appropriate warning messages.
5. The Anti-Virus solution should scan all compressed file formats.
6. The Anti-Virus Solution should provide a feature for the rollback of malware actions during disinfection (Rollback means rolling back the changes made to the file system creating, relocating, re-naming of files and registry keys).
7. The Anti-Virus should provide web Anti-Virus features which should analyse site address and block access to dangerous sites and scan the object downloaded over HTTP.
8. The Anti-Virus Solution should provide mail Anti-Virus features which should protect from the threats that email messages may contain and messages should be intercepted.
9. The Anti-Virus Solution should provide temper protection features i.e. the user, who does not know the password, should not be able to change the existing policy, exit or uninstall the Anti-Virus solution.
10. The Anti-Virus Solution should have profile based policies i.e. users should be categorised based on profile and necessary policies should be applied to this profile. Any change in profile/policy should reflect on the users of that profile. The Administrator should be able to move the users between different profiles.
11. Alerts on virus activity should be passed on to the administrator.
12. Anti-Virus Solution should provide web control module with the ability to monitor and filter users' browser activities by category, content and data type regardless of workstation location.
13. Vendor should have 24x7 anti-malware laboratory analysis centres to provide proactive rapid protection against the known and unknown threats.
14. The Anti-virus Solution should have a mechanism to issue and withdraw licenses from a PC/Server as the existing PCs/Servers may be scrapped or new PCs/Servers may be procured during the year.

15. The Anti-Virus Solution Server to be installed on premise and the quote should be for an on-premise based solution.

T.2 : Optional.

1. The Anti-Virus Solution should have deep/machine learning technology to block zero day malware.
2. The Anti-Virus Solution should be able to detect vulnerabilities in installed Software/Applications on the client.

MORMUGAO PORT TRUST

ANNEXURE B

TECHNICAL COMPLIANCE OF ANTI-VIRUS & ENDPOINT PROTECTION SOLUTION

Sr. No.	Feature Required	Indicate whether Supports - Yes/No
1.0	Enterprise Control	
1.1	Platform supported (List 1) : Windows SBS 201/ Windows Server 2003 and R2/ Windows Server 2008 and R2/ Windows Server 2012 and R2/ Windows Server 2016	
1.2	Database Platforms supported: SQL Express Edition	
1.3	Virtualization platforms are supported (Vmware and Hyper -V)	
1.4	Ability to deploy, update, configure and monitor clients with centralized administration of all Endpoint Protection components on simple and complex networks	
1.5	All settings for Endpoint Protection Advanced will be be configured from Enterprise Console without the need to access additional consoles	
1.6	Must have integrated reporting that delivers instant and scheduled report of the threat alerts, infections and at-a-glance report for outbreak risk. Support report output in PDF, HTML, Excel, Word, RTF, CSV, XML.	
2.0	Policy-Based	
2.1	Must have policy-based management; centralized policy covering updating schedules, antivirus and HIPS, client firewall, application, device and data control and more	
2.2	Centralized policy covering updating schedules, Antivirus and HIPS, client firewall, application, device and data control	
2.3	Can create subgroups (sub-estates) to create an entire tree, all subgroups inherit the policies applied to the parent group	
3.0	Role-Based Administration	
3.1	Have the capability to allow the separation of estate management to different administrator login	
3.2	Delegate part of the administration to a list of administrators with restricted permissions.	
3.3	Can create custom roles that will suit to needs and can be are assigned to Windows users or Windows groups.	

4.0	Tamper Protection	
4.1	Prevents users from uninstalling the antivirus, auto update, client firewall, remote management system and disk encryption on a windows computer	
4.2	Policy is configured within Enterprise Console	
4.3	Requires password to be set for protection and can only be configured on the endpoint if the user has administration rights or the correct password is entered.	
5.0	Dashboard and Reporting	
5.1	Integrated graphical reporting delivers instant and scheduled email report of the threat alerts and infections while the security dashboard gives an at-a-glance report for outbreak risk	
5.2	Near real-time view of the security health of the organization through the use of dashboards or similar technology	
5.3	Automated email reporting when certain alert threshold is reached	
5.4	Support report output in PDF, HTML, Excel, Word, RTF, CSV, XML	
6.0	Signature Updates	
6.1	Small update size with an average of 50KB per signature update	
6.2	Ability to check for updates as often as every 20 minutes if not continues	
6.3	Separate schedule for signature and software updates	
7.0	Endpoint Protection	
7.1	Platform Supported: - Win XP/Vista/Win 7 including XP mode/Win 8/Win 8.1/Win 10 - Win SBS 2011/Server 2008 including Core/Server R2 including Core/Server 2012 including Core/Server 2012 R2 including Core/Server 2016/ - VMware Sphere/ESX//Hyper V/Citrix Xen Server - MAC OS/Linux	
7.2	Microsoft Active Directory synchronization - Automatic computer discovery and synchronization with AD structure - Automatic installation of newly discovered endpoint	
7.3	Endpoint discovery (with and without agent; active and inactive devices)	
7.4	Deployment Options - Use the protect computer wizard - Active Directory synchronization - Push deployment via script - Manual (Locate installers for protecting computers manually)	
7.5	Actionable security dashboard can perform full scan, cleanup and remediation	
7.6	Monitors applications launched on the endpoints, removable devices and data that are forwarded or transmitted	

7.7	Monitor and control suspicious behavior like registry or critical windows system files modification	
7.8	Rootkit detection and cleanup	
7.9	Detects, block and clean up known and unknown threats, included virus, spyware, adwares and PUAs	
7.10	Antivirus with Intercheck technology	
7.11	Intercepts and scans files as they are accessed	
7.12	Assess computers for missing patches	
8.0	Client Firewall	
8.1	Platform supported: Win XP/Vista/Windows 7/Windows 8/Windows 8.1/Windows 10	
8.2	Provides stealth mode	
8.3	Prevents application hijacking and checksum-based exclusion	
8.4	Centrally Managed Firewall	
8.5	Have location-aware feature (apply different firewall policies when endpoint is within or outside network)	
8.6	Integrated with endpoint protection agent	
8.7	Have the ability to be set in stealth mode	
8.8	Use " stateful inspection " and monitor communication between packets	
9.0	Application Control	
9.1	Selectively authorize or block legitimate Applications that impact network bandwidth, Systems availability, and user productivity	
9.2	Integrated with endpoint protection agent	
9.3	Monitor applications launched on the endpoints, removable devices and data that are forwarded or transmitted	
9.4	Vendor-managed list to offload the administrator from monitoring new applications or versions Administrators can select and allow specific applications or specific categories of applications.	
9.5	Provides and automatically updates the list of controlled applications	
9.6	Integrated in unified detection engine	
9.7	Policy set in central management console	
9.8	Allows different policies for different groups	
9.9	Can enforce company policies as well as reduce security risks.	
9.10	Stop instant messaging, games, peer-to-peer applications who consume bandwidth.	
9.11	Prevent confidential information from being exposed via peer-to-peer exchange or transmitted via instant messaging	
10.0	Device Control	
10.1	Control the use of removable storage, optical media drives and wireless networking devices and define which computers have access to specific removable devices	

10.2	integrated with endpoint protection agent	
10.3	Should be port-agnostic and should support whatever port is used to connect the device like USB, FireWire, SATA and PCMCIA interfaces	
10.4	able to control the use of Media Transfer Protocol (MTP) and Picture Transfer Protocol (PTP) devices, removable storage, optical media drives and wireless networking devices	
10.5	Ability to set storage devices in "Read-only mode" to prevent data from being written	
10.6	Must prevent wireless bridging (ex. Disables wireless when Ethernet is connected protecting our network from backdoor connections)	
10.7	Supports device instance and model exceptions	
10.8	Easy authorization of allowed devices	
10.9	Integrated in unified detection engine	
10.10	Policy set in central management console	
10.1	Allows different policies for different groups	
10.12	Block Windows from bridging two networks	
11.0	Host Intrusion Prevention System (HIPS)	
11.1	Guarding against unknown threats by analyzing behaviour before code executes	
11.2	integrated with endpoint protection agent	
11.3	Stop zero-day threats with built-in HIPS Behavioural Protection	
11.4	Suspicious Behaviour Detection	
11.5	Buffer Overflow Protection	
12.0	Runtime Protection	
12.1	Monitor and block suspicious behaviour like registry or critical windows system files modification	
12.2	Protection against buffer overflow	
13.0	Web Protection	
13.1	Block URLs that are hosting malware	
13.2	Live in-the-cloud lookups check database of Millions of compromised sites	
13.3	Protects users everywhere, in the office, and when not behind corporate protection, i.e. at home or over public WIFI	
13.4	Integrated into existing endpoint agent with no endpoint configuration required	
13.5	Online scanning for malware (in the cloud)	
13.6	Runtime HIPS/behaviour combination	
13.7	Ability to detect and block compromised / hijacked trusted sites	
13.8	Multi-web browser support	
13.9	Provides control of the Internet regardless of the browser used through "Web LENS" technology (Web Lightweight Endpoint Scanner).	

14.0	Data Loss Prevention	
14.1	Data Loss protection	
14.2	Control the transfer of sensitive data	
14.2	Integrated into endpoint agent	
14.3	Pre-packaged data definitions	
14.4	Integrated in the license	
15.0	Data Control	
15.1	Must be fully integrated content monitoring solution	
15.2	Monitors data transferred onto data points like removable storage, optical and disk drives, and internet-enabled applications (web browser, email client, instant messaging)	
15.3	Block/allow/warn/log transfer of files based on "true" file type and/or content using regular expressions	
15.4	Integrated in the license / endpoint agent	
15.5	Control the transfer of sensitive data	
15.6	Pre-packaged data definitions of sensitive and personally identifiable information (PII) to save time	
15.7	Monitor transfer of sensitive data to removable storage.	
16.0	Web Control	
16.1	Control access inappropriate website	
16.2	Create Web control policy from enterprise console and apply to the right PC group	
16.3	Add own list of URLs or IP address via exceptions tab	

Note : Please include Annexure B complete in all respects duly signed and sealed in Technical Bid Cover.

MORMUGAO PORT TRUST**DETAILS FOR SUBMISSION BY VENDORS ALONG WITH TENDER.****A. VENDOR DETAILS OF VENDOR**

1.	Name of the Organisation	
2.	Address (in detail)	
3.	Telephone no.	
4.	E-mail ID	
5.	PAN No.	
6.	Tax Identification No. (TIN)	
7.	Service Tax Registration No.	
8.	Service Tax Registration Code	
9.	CST Registration No.	
10.	Employee Provident Fund (PPF)	
11.	Employee State Insurance Scheme (ESIC) Registration No.	

B. BANK DETAILS OF VENDORS.

1.	Bank Name	
2.	Bank Branch Address (in detail)	
3.	Bank Branch Code	
4.	Bank Account No.	
5.	Bank Account Type	
6.	Magnetic Ink Character Recognizer (MICR)	
7.	IFSC Code.	

MORMUGAO PORT TRUST
ELECTRONIC PAYMENT SYSTEM MANDATE FORM

The details for processing the payment through RTGS as below:-

Name of the Beneficiary	MORMUGAO PORT TRUST
Address of Beneficiary with PIN Code	Administrative Office Building, Headland Sada, GOA - 403804
PAN Number	AAALMO293P
Name & Mobile Number of responsible person	RAGHUNATH MORAJKAR / 9423059702 raghunath.morajkar@mptgoa.com
Name of the Bank and Branch	STATE BANK OF INDIA, Harbour Branch
Bank Telephone No.	0832-2520212
Address of the Bank	STATE BANK OF INDIA MORMUGAO HARBOUR, GOA – 403803
MICR Code of the Bank	403002024
IFSC Code No.	SBIN0002164
Type of Account and Branch Code	Current Account / Branch Code:- 002164
Account number of the Bank	10438017048
Beneficiary E-mail ID	cashmpt@mptgoa.com

MORMUGAO PORT TRUST**GST PARTICULARS TO BE FURNISHED BY BIDDER IF APPLICABLE**

Sr No	Particular	Mormugao Port Trust	Data Required
1	Customer Name as per GST Registration Certificate	Mormugao Port Trust	
2	Full Postal Address	Administrative Building, Headland Sada.	
3	City	Goa	
4	Pin code	403 804	
5	PAN	AAALM0293P	
6	Type of Person	Local Authority	Company/Firm/Individual/Trust/LLP/AOP
7	Resident/Non Resident as per Income Tax Act	Resident	
8	ARN No.	AA30617001663N	
9	GST No.	30AAALM0293P1ZY	
10	PPOB (Principal Place of Business) or APOB (Additional Place of Business)	PPOB	
11	Reason for Non Registration (Turnover Limit / Non Taxable Supply / Other Reason)	NA (Registered Under GST)	
12	Type of Customer (Manufacturer/Trader/Importer/ Depot/Service Provider/Works Contractor/Principal/Consumer)	Service Provider	
13	Whether Falling under SEZ unit or Developer? (Yes or No)	No.	
14	Whether B2B or B2c (B= Business & C= Customer)	B2B	
15	Whether Opted for Composition Lavy Scheme? (Yes or No)	No.	
16	Whether falling under casual taxable person as per Section 2(20) of CGST Act,2017 (yes or No)	No.	
17	Whether falling under Non Resident taxable person as per section 2(77) of CGST Act, 2017 ? (Yes or No)	No.	

18	Central Excise Registration No.	--	
19	Service Tax Registration No.	AAALM0293PST0 01	
20	VAT - TIN	30181201096	
21	CST - TIN	V/CST/1683	
22	IEC	1706000073	
23	Contact Details :		
	Name	Shri. Anant Chodnekar	
	Designation	Sr. Dy.CAO	
	Phone No.	0832-2521132	
	E-mail	facao@mptgoa.com m anant.chodnekar @mptgoa.com	